



**Universidad Nacional Autónoma de México**

**ANEXOS DE LAS NORMAS COMPLEMENTARIAS SOBRE MEDIDAS DE SEGURIDAD  
TÉCNICAS, ADMINISTRATIVAS Y FÍSICAS PARA LA PROTECCIÓN  
DE DATOS PERSONALES EN POSESIÓN DE LA UNIVERSIDAD**



**DOCUMENTO DE SEGURIDAD**

Índice

Presentación

Introducción

Sistemas de tratamiento de datos personales

1. Inventario de sistemas de tratamiento de datos personales
2. Estructura y descripción de los sistemas de tratamiento de datos personales
3. Análisis de riesgos
4. Análisis de brecha
5. Plan de trabajo
6. Medidas de seguridad implementadas
7. Mecanismos de monitoreo y revisión de las medidas de seguridad
8. Programa específico de capacitación
9. Mejora continua
10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales
11. Aprobación del documento de seguridad

## **Presentación**

El 11 de junio por acuerdo del rector desaparecen la Coordinación de Desarrollo Educativo e Innovación Curricular, dependiente de la Secretaría General, y la Coordinación de Universidad Abierta y Educación a Distancia, dependiente de la Secretaría de Desarrollo Institucional y se crea la Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED), dependiente de la Secretaría General. Contará con una persona titular que tendrá el cargo de Coordinador, nombrado y removido libremente por la o el Secretario General.

La CUAIEED es la Coordinación encargada de consolidar el desarrollo y evaluación de la educación en la Universidad, en todas sus modalidades, para articular políticas, programas, acciones y estrategias de la educación universitaria.

## **Introducción**

El presente documento de seguridad contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales de esta área universitaria con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Su propósito es identificar los sistemas de tratamiento de datos personales que posee esta área universitaria, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

Este modelo pretende brindar a las áreas universitarias homogeneidad en la redacción, organización y contenido para que elaboren su propio documento de seguridad en el que se describen las tres medidas de seguridad para la protección de los datos personales.

El marco jurídico del documento de seguridad se regula por el capítulo II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada el 26 de enero de 2017, que establece un conjunto mínimo de medidas de seguridad que cada dependencia o entidad universitaria deberá considerar al perfilar su estrategia de seguridad para la protección de los datos personales bajo su custodia, según el tipo de soportes —físicos, electrónicos o ambos— en los que residen dichos datos y dependiendo del nivel de protección que tales datos requieran.

Específicamente los artículos 31, 32 y 33 de la Ley General, del 55 al 72 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018, así como del 20 al 31 de los Lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México, publicados en la Gaceta UNAM el 25 de febrero de 2019.

El cimiento del formato de documento de seguridad es la aplicación de un enfoque basado en los riesgos de los activos universitarios, específicamente los datos personales y los soportes que los resguardan. Además, el formato considera el tamaño y estructura de la institución, objetivos, clasificación de la información, requerimientos de seguridad y procesos que se precisan en razón de los activos que posee esta Máxima Casa de Estudios, lo cual se encuentran contemplado en el estándar internacional en materia de seguridad de la información ISO/IEC 27002:2013 "*Tecnología de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información*".

## Sistemas de Tratamiento de Datos Personales

La Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED) cuenta con varios sistemas que apoyan a la gestión de procesos de diferentes áreas, entidades y dependencias dentro de la UNAM, en los cuales se hace tratamiento de datos personales de trabajadores, docentes y alumnos.

Los sistemas que hacen tratamiento de datos se enlistan a continuación:

<b>Identificador único</b>	<b>Nombre del sistema</b>
CUAIEED-DBDyM-01	Comunidad Premed
CUAIEED-DBDyM-02	Comunidad PreFA
CUAIEED-DBDyM-03	Comunidad Prevet
CUAIEED-DBDyM-04	Esp BUNAM
CUAIEED-DBDyM-05	Guía Educativa IME
CUAIEED-DDSE-01	Sistema de Gestión de Constancias (SIGECO)
CUAIEED-DDSE-02	Encuestas CUAIEED - Limesurvey
CUAIEED-DDSE-03	Piensa Más Allá
CUAIEED-DDSE-04	Argumente
CUAIEED-DDSE-05	Sistema de Información y Control Escolar (SIICOE)
CUAIEED-DDSE-06	Sistema de Administración y Seguimiento de Proyectos (SASP)
CUAIEED-DDSE-07	Aulas Virtuales
CUAIEED-DDSE-08	DespegApp
CUAIEED-DDSE-09	Moodle
CUAIEED-DDSE-10	Drupal
CUAIEED-DIEDCFD-001	Sistema de Gestión de Formación Docente
CUAIEED-DIEDCFD-002	Tienda Virtual CUAIEED
CUAIEED-DIEDCFD-003	Sistema de Registro - Jornada de Formación Docente
CUAIEED-DIEDCFD-004	Catálogo de Insumos Audiovisuales Didácticos Digitales
CUAIEED-DIEDCFD-005	Resultados de Evaluación de Actividades de Formación Docente
CUAIEED-DIEDCFD-006	Sistema de Encuesta de Formación Docente

CUAIEED-DEE-001	Sistema Integral de Gestión de Exámenes (SIGE)
CUAIEED-DEE-002	Repositorio Digital
CUAIEED-DEE-003	Sistema de Aprendizaje de Bachillerato en Red (SABER)
CUAIEED-DEE-004	Pruébate UNAM Licenciatura
CUAIEED-DEE-005	Pruébate UNAM Bachillerato
CUAIEED-DEE-006	Diseño y Aplicación de Exámenes (DAEX)
CUAIEED-DEE-007	Sistema de Análisis Psicométrico de Reactivos (SISAPRE)
CUAIEED-DEE-008	Exámenes en Línea (EXAL)
CUAIEED-DEE-009	Sistema de Planes y Programas de Estudio
CUAIEED-DEE-010	Sistema de Evaluación Docente
CUAIEED-DEE-011	Sistema de Gestión de Concursos
CUAIEED-DEE-012	Plataforma Moodle Comisión Especial de Lenguas
CUAIEED-DEE-013	Open Journal System Revista Digital Universitaria Revista de Investigación en Educación Médica
CUAIEED-DEE-014	Plataforma LimeSurvey Seguimiento de egresados
CUAIEED-DEE-015	Plataforma Wordpress Comunidad de Educación Basada en Evidencias
UNAM:6C.13/482-63"2022"	Sistema Institucional de Compras
Sistema Integral de Personal (SIP)	Sistema Integral de Personal (SIP)
UNAM:4C.14/482-2022	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios.
Apl_482 (//172.16.3.150) (z)	Sistema Integral de Administración Financiera
UNAM:7C.1/482	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma.

## Comunidad Premed

### Introducción

La plataforma Comunidad Premed sirve a estudiantes de primer ingreso a la Facultad de Medicina de la UNAM y Universidad de la Salud de la Secretaría de Educación, Ciencia, Tecnología e Innovación de la Ciudad de México, así como público en general que tienen interés en fortalecer sus conocimientos base para tener un buen desempeño en su tránsito por el primer año de la licenciatura, al contar con cursos enfocados en temas del área tronco común del área de las ciencias biológicas y de la salud. Los usuarios tienen la posibilidad de hacer una prueba inicial por curso para conocer su nivel actual y realizar otra prueba al final del curso para conocer la mejora en su desempeño.

### 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección de Bachillerato a Distancia y Mooc</b>	
<b>Identificador único*</b>	CUAIEED-DBDyM-01
<b>Nombre del sistema A1*:</b>	<b>Comunidad Premed</b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre, correo electrónico (personal o institucional), género, fecha de nacimiento, escuela de procedencia
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
<b>Nombre*:</b>	Dra. Guadalupe Vadillo Bueno
<b>Cargo*:</b>	Directora de Bachillerato a distancia y MOOC
<b>Funciones*:</b>	Dirección de proyectos educativos de impacto en el programa de Bachillerato a distancia y proyectos externos.
<b>Obligaciones*:</b>	<ul style="list-style-type: none"><li>- Definir junto con los usuarios del sistema, los tipos de acceso.</li><li>- Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.</li></ul>
	<b>Encargados:</b>
<b>(Nombre del Encargado 1*:</b>	Mtro. Alan López de Jesús
<b>Cargo*:</b>	Jefe de Área del Departamento de Operaciones y Seguridad Informática.
<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.

<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 2*:</b>	Mtro. Enrique Tezozomoc Pérez Campos
<b>Cargo*:</b>	Jefe del Departamento de Operaciones y Seguridad Informática
<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 3*:</b>	Mtro. <a href="#">Omar Terrazas Razo</a>
<b>Cargo*:</b>	Coordinador de Bachillerato a distancia
<b>Funciones*:</b>	Coordinador de Bachillerato a distancia y del desarrollo de materiales y sistemas educativos a través de la coordinación del Laboratorio de Arte y Tecnología.
<b>Obligaciones*:</b>	Procurar la protección de los datos personales contenidos en el sistema.
	<b>Usuarios:</b>
<b>(Nombre del Usuario *)</b>	Facultad de Medicina de la UNAM, Universidad de la Salud de la Secretaría de Educación, Ciencia, Tecnología e Innovación de la Ciudad de México y público en general.
<b>Cargo*:</b>	Comunidad académica y estudiantil.
<b>Funciones*:</b>	Consultar el contenido de la plataforma, realizar evaluaciones diagnósticas de los cursos que contiene el sitio y evaluaciones para medir su desempeño dentro de la plataforma.
<b>Obligaciones*:</b>	Validar que la información que se distribuye dentro del sistema no contenga datos personales visibles de la comunidad universitaria o un tercero.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

**Dirección de Bachillerato a Distancia y Mooc**

<b>Identificador único*</b>	CUAIEED-DBDyM-01
<b>(Nombre del sistema A1*)</b>	Comunidad Premed
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos
<b>Características del lugar donde se resguardan los soportes: *</b>	

### 3. ANÁLISIS DE RIESGOS

Dirección de Bachillerato a Distancia y Mooc

Identificador único\* CUAIEED-DBDyM-01

(Nombre del sistema A1) \* Comunidad Premed

Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado.	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor.
Explotación de vulnerabilidades.	Medio	Actualización del core del aplicativo desarrollado en PHP Codeigniter.
Librerías de terceros.	Medio	Actualización de librerías NodeJS que se encuentran en el frontend y realizan las peticiones al backend.

### 4. ANÁLISIS DE BRECHA

Dirección de Bachillerato a Distancia y Mooc



Identificador único*	CUAIEED-DBDyM-01	
Nombre del sistema A1) *	Comunidad Premed	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Cifrado de comunicaciones entre cliente y servidor.	Uso de certificado de seguridad SSL/TLS en todas las comunicaciones realizadas por la plataforma.	Uso en local de imágenes y librerías javascript empleadas en el frontend.
Actualización de la plataforma.	Trabajar sobre la última versión estable del framework Codeigniter y Node.JS.	Reducir los tiempos requeridos para mantener la plataforma actualizada.

## 5. PLAN DE TRABAJO

Dirección de Bachillerato a Distancia y Mooc			
Identificador único*	CUAIEED-DBDyM-01		
(Nombre del sistema A1) *	Comunidad Premed		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización a la última versión estable del framework	La actualización de la plataforma permite mantener el código fuente en su última versión, con esta actividad se protege la integridad de los datos contenidos en esta.	15 días	Total.

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

<b>Dirección de Bachillerato a Distancia y Mooc</b>	
<b>Identificador único*</b>	CUAIEED-DBDyM-01
<b>(Nombre del sistema A1) *</b>	<b>Comunidad Premed</b>
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
<b>Transferencias mediante el traslado de soportes físicos:</b>	No se realiza tratamiento de datos personales con soportes físicos, se tiene soporte electrónico en una base de datos.
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias mediante el traslado de soportes electrónicos.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No se realizan transferencias mediante el traslado sobre redes electrónicas.

### **I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

No aplica, se tiene soporte electrónico en una base de datos.

### **II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web y la base de datos de la plataforma, almacenando la fecha, hora, dirección IP, así como todas las acciones dentro del servidor que la aloja. Los archivos de log que se encuentran dentro del sistema operativo se rotan cada diez días mientras que las bitácoras dentro de la base de datos se almacenan de forma indeterminada hasta el final de la vida útil del sistema. La integridad de las bitácoras se garantiza utilizando una suma de HASH. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática, las herramientas utilizadas para el análisis son AWK, SED y GREP.

### **III. REGISTRO DE INCIDENTES**

Los incidentes son reportados al Departamento de Operaciones y Seguridad Informática en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuenta con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

El tipo de soporte es electrónico por lo que la recuperación de la base de datos, la cual se encarga de almacenar los datos personales de los usuarios, es el proceso más importante. Este consiste en recuperar la copia de la base de datos obtenida en el proceso de respaldo programado.

### **V. ACCESO A LAS INSTALACIONES**

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente. La dependencia se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

El procedimiento para actualizar o corregir datos personales se encuentra indicado dentro de la plataforma, información disponible únicamente para el usuario registrado, y el cual consiste en entrar a su perfil y actualizar la información de los campos que se encuentran disponibles en el formulario. En el caso de actualización de nombre, correo electrónico o número de cuenta debe solicitarlo vía correo electrónico a la dirección [premed@cuaieed.unam.mx](mailto:premed@cuaieed.unam.mx).

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

Los perfiles de usuario en esta plataforma únicamente permiten separar el tipo de usuario de manera estadística pero no implica algún cambio en los permisos o funciones de la plataforma. El sistema de cuentas de usuario local cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible utilizando MD5.

Existe un tipo de usuario que tiene acceso únicamente a información estadística relacionada con el desempeño de los estudiantes, omitiendo la información de nombre, correo electrónico y número de cuenta. El acceso a estas consultas se realiza desde un sitio independiente que no se encuentra enlazado desde el sitio principal de la plataforma.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

Las plataformas son respaldadas utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello, por un promedio de treinta días tras, y almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas seguras y en condiciones óptimas para su funcionamiento. Para promover la conservación y preservación de la información, las cintas y el lector de estas se mantienen por tiempo indefinido.

## **IX. PLAN DE CONTINGENCIA**

Se cuenta con un plan de contingencia que permite la continuidad de negocio, el cual utiliza como fuente primordial los respaldos obtenidos de las plataformas en cintas magnéticas y en un servidor dedicado. Las pruebas de eficiencia que se realizan han garantizado la recuperación total de la plataforma en un periodo máximo de doce horas. Actualmente no se cuenta con un sitio redundante o alterno.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1. Herramientas y recursos para monitoreo de la protección de datos personales

[Redacted content]		
[Redacted content]	[Redacted content]	
[Redacted content]	[Redacted content]	
[Redacted content]	[Redacted content]	[Redacted content]
[Redacted content]	[Redacted content]	[Redacted content]

### 7.2. Procedimiento para la revisión de las medidas de seguridad

[Redacted content]		
[Redacted content]	[Redacted content]	
[Redacted content]	[Redacted content]	
[Redacted content]	[Redacted content]	[Redacted content]
[Redacted content]	[Redacted content]	[Redacted content]


### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección de Bachillerato a Distancia y Mooc		
<b>Identificador único*</b>	CUAIEED-DBDyM-01	
<b>(Nombre del sistema A1) *</b>	Comunidad Premed	
<b>Medida de seguridad*</b>	<b>Resultado de evaluación*</b>	<b>Responsable*</b>
<i>Revisión de permisos.</i>	<i>Se cuentan con los permisos adecuados.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática.</i>
<i>Script de respaldos de información.</i>	<i>Los respaldos funcionan correctamente.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática.</i>
<i>Actualización del sistema operativo.</i>	<i>Se cuentan con las últimas actualizaciones.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática.</i>

<i>Actualización de la aplicación.</i>	<i>Actualización de framework y librerías de frontend.</i>	<i>Responsable: Coordinación de Bachillerato a distancia.</i>
--	--	---

#### 7.4. Acciones para la corrección y actualización de las medidas de seguridad


#### 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

##### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

**No se cuenta con un programa formal de capacitación**

**8.2. Programa de difusión de la protección a los datos personales**  
*(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)*

**No se tiene un programa de difusión de la protección a los datos personales**

#### 9. MEJORA CONTINUA

##### 9.1. Actualización y mantenimiento de sistemas de información

Dirección de Bachillerato a Distancia y Mooc			
<b>Identificador único*</b>	CUAIEED-DBDyM-01		
<b>(Nombre del sistema A1) *</b>	Comunidad Premed		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
<i>Actualización de la plataforma a nuevas versiones.</i>	<i>Proceso de actualización hacia versiones superiores del framework Codeigniter y NodeJS.</i>	<i>1 mes.</i>	<i>Total.</i>

### 9.2. Actualización y mantenimiento de equipo de cómputo

Dirección de Bachillerato a Distancia y Mooc			
<b>Identificador único*</b>	CUAIEED-DBDyM-01		
<b>(Nombre del sistema A1*):</b>	Comunidad Premed		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
<i>Actualización del servidor físico.</i>	<i>Cambio del servidor físico utilizado para crear máquinas virtuales donde se hospeda la plataforma.</i>	<i>3 años.</i>	<i>Total.</i>

### 9.3. Procesos para la conservación, preservación y respaldos de información

Dirección de Bachillerato a Distancia y Mooc			
--	--	--	--

<b>Identificador único*</b>	CUAIEED-DBDyM-01	
<b>(Nombre del sistema A1*:</b>	<b>Comunidad Premed</b>	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
<i>Resguardo de cintas magnéticas.</i>	<i>Las cintas magnéticas realizadas en la fase de respaldo automatizado y el lector de las cintas magnéticas son resguardadas de forma indefinida.</i>	<i>Departamento de Operaciones y Seguridad Informática.</i>

#### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

<b>Dirección de Bachillerato a Distancia y Mooc</b>		
<b>Identificador único*</b>	CUAIEED-DBDyM-01	
<b>(Nombre del sistema A1*:</b>	<b>Comunidad Premed</b>	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
<i>Borrado seguro.</i>	<i>Se realiza un formato de bajo nivel al disco duro físico del hipervisor.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.</i>

### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La Dirección de Bachillerato a Distancia y Mooc recibe o envía la petición en donde se indica la razón para la cancelación del sistema, el tiempo que deberá de permanecer la plataforma funcionando antes de ser eliminada y si se necesita entregar un respaldo final del sistema para su resguardo final en un soporte electrónico. La petición siempre es en formato escrito ya sea por correo electrónico o por oficio. El sistema será eliminado tras una fecha de término establecida y se borra de forma permanente la máquina virtual donde este reside.

#### Comunidad PreFA



## Introducción

La plataforma Comunidad PreFA sirve a estudiantes de primer ingreso a la Facultad de Arquitectura de la UNAM, así como público en general que tienen interés en fortalecer sus conocimientos base para tener un buen desempeño en su tránsito por el primer año de la licenciatura, al contar con cursos enfocados en temas del tronco común del área de las ciencias fisicomatemáticas, lectura y redacción y estrategias de aprendizaje en línea. Los usuarios tienen la posibilidad de hacer una prueba inicial por curso para conocer su nivel actual y realizar otra prueba al final del curso para conocer la mejora en su desempeño.

### 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección de Bachillerato a Distancia y Mooc</b>	
<b>Identificador único*</b>	CUAIEED-DBDyM-02
<b>Nombre del sistema A1*:</b>	<b>Comunidad PreFA</b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre, correo electrónico (personal o institucional), genero, fecha de nacimiento, escuela de procedencia
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
<b>Nombre*:</b>	Dra. Guadalupe Vadillo Bueno
<b>Cargo*:</b>	Directora de Bachillerato a distancia y MOOC
<b>Funciones*:</b>	Dirección de proyectos educativos de impacto en el programa de Bachillerato a distancia y proyectos externos.
<b>Obligaciones*:</b>	<ul style="list-style-type: none"> <li>- Definir junto con los usuarios del sistema, los tipos de acceso.</li> <li>- Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.</li> </ul>
	<b>Encargados:</b>
<b>(Nombre del Encargado 1*:</b>	Mtro. Alan López de Jesús
<b>Cargo*:</b>	Jefe de Área del Departamento de Operaciones y Seguridad Informática.
<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.

<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 2*:</b>	Mtro. Enrique Tezozomoc Pérez Campos
<b>Cargo*:</b>	Jefe del Departamento de Operaciones y Seguridad Informática
<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 3*:</b>	Mtro. Omar Terrazas Razo
<b>Cargo*:</b>	Coordinador de Bachillerato a distancia
<b>Funciones*:</b>	Coordinador de Bachillerato a distancia y del desarrollo de materiales y sistemas educativos a través de la coordinación del Laboratorio de Arte y Tecnología.
<b>Obligaciones*:</b>	Procurar la protección de los datos personales contenidos en el sistema.
	<b>Usuarios:</b>
<b>(Nombre del Usuario *)</b>	Facultad de Arquitectura de la UNAM y público en general.
<b>Cargo*:</b>	Comunidad académica y estudiantil.
<b>Funciones*:</b>	Consultar el contenido de la plataforma, realizar evaluaciones diagnósticas de los cursos que contiene el sitio y evaluaciones para medir su desempeño dentro de la plataforma.
<b>Obligaciones*:</b>	Validar que la información que se distribuye dentro del sistema no contenga datos personales visibles de la comunidad universitaria o un tercero.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección de Bachillerato a Distancia y Mooc</b>	
<b>Identificador único*</b>	CUAIEED-DBDyM-02

<b>(Nombre del sistema A1*)</b>	Comunidad PreFA
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos
<b>Características del lugar donde se resguardan los soportes: *</b>	Alojamiento en el centro de datos de CUAIEED dentro de diversas máquinas virtuales, el cual cuenta con acceso mediante un sistema biométrico, planta de energía eléctrica, sistema de respaldo de energía eléctrica ininterrumpida (UPS) y aire acondicionado seco.

### 3. ANÁLISIS DE RIESGOS

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-02	
Nombre del sistema A1*	Comunidad PreFA	
<b>Riesgo*</b>	<b>Impacto*</b>	<b>Mitigación*</b>
Ingreso no autorizado	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor.
Explotación de vulnerabilidades	Medio	Actualización del core del aplicativo desarrollado en PHP Codeigniter.
Librerías de terceros	Medio	Actualización de librerías NodeJS que se encuentran en el frontend y realizan las peticiones al backend.

### 4. ANÁLISIS DE BRECHA

Dirección de Bachillerato a Distancia y Mooc		
--	--	--

Identificador único*	CUAIEED-DBDyM-02	
Nombre del sistema A1) *	Comunidad PreFA	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Cifrado de comunicaciones entre cliente y servidor.	Uso de certificado de seguridad SSL/TLS en todas las comunicaciones realizadas por la plataforma.	Uso en local de imágenes y librerías javascript empleadas en el frontend.
Actualización de la plataforma.	Trabajar sobre la última versión estable del framework Codeigniter y Node.JS.	Reducir los tiempos requeridos para mantener la plataforma actualizada.

## 5. PLAN DE TRABAJO

Dirección de Bachillerato a Distancia y Mooc			
Identificador único*	CUAIEED-DBDyM-02		
(Nombre del sistema A1) *	Comunidad PreFA		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización a la última versión estable del framework	La actualización de la plataforma permite mantener el código fuente en su última versión, con esta actividad se protege la integridad de los datos contenidos en esta.	15 días	Total.

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

<b>Dirección de Bachillerato a Distancia y Mooc</b>	
<b>Identificador único*</b>	CUAIEED-DBDyM-02
<b>(Nombre del sistema A1) *</b>	<b>Comunidad PreFA</b>
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
<b>Transferencias mediante el traslado de soportes físicos:</b>	No se realiza tratamiento de datos personales con soportes físicos, se tiene soporte electrónico en una base de datos.
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias mediante el traslado de soportes electrónicos.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No se realizan transferencias mediante el traslado sobre redes electrónicas.

### **I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

No aplica, se tiene soporte electrónico en una base de datos.

### **II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web y la base de datos de la plataforma, almacenando la fecha, hora, dirección IP, así como todas las acciones dentro del servidor que la aloja. Los archivos de log que se encuentran dentro del sistema operativo se rotan cada diez días mientras que las bitácoras dentro de la base de datos se almacenan de forma indeterminada hasta el final de la vida útil del sistema. La integridad de las bitácoras se garantiza utilizando una suma de HASH. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática, las herramientas utilizadas para el análisis son AWK, SED y GREP.

### **III. REGISTRO DE INCIDENTES**

Los incidentes son reportados al Departamento de Operaciones y Seguridad Informática en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuenta con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

El tipo de soporte es electrónico por lo que la recuperación de la base de datos, la cual se encarga de almacenar los datos personales de los usuarios, es el proceso más importante. Este consiste en recuperar la copia de la base de datos obtenida en el proceso de respaldo programado.

### **V. ACCESO A LAS INSTALACIONES**

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente. La dependencia se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el director de la Dirección de Desarrollo de Sistemas para la Educación.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

El procedimiento para actualizar o corregir datos personales se encuentra indicado dentro de la plataforma, información disponible únicamente para el usuario registrado, y el cual consiste en entrar a su perfil y actualizar la información de los campos que se encuentran disponibles en el formulario. En el caso de actualización de nombre, correo electrónico o número de cuenta debe solicitarlo vía correo electrónico a la dirección [bunam\\_apps@cuaieed.unam.mx](mailto:bunam_apps@cuaieed.unam.mx).

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

Los perfiles de usuario en esta plataforma únicamente nos permiten separar el tipo de usuario de manera estadística pero no implica algún cambio en los permisos o funciones de la plataforma. El sistema de cuentas de usuario local cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible utilizando MD5.

Existe un tipo de usuario que tiene acceso únicamente a información estadística relacionada con el desempeño de los estudiantes, omitiendo la información de nombre, correo electrónico y número de cuenta. El acceso a estas consultas se realiza desde un sitio independiente que no se encuentra enlazado desde el sitio principal de la plataforma.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

Las plataformas son respaldadas utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello, por un promedio de treinta días tras, y almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas seguras y en condiciones óptimas para su funcionamiento. Para promover la conservación y preservación de la información, las cintas y el lector de estas se mantienen por tiempo indefinido.

## **IX. PLAN DE CONTINGENCIA**

Se cuenta con un plan de contingencia que permite la continuidad de negocio, el cual utiliza como fuente primordial los respaldos obtenidos de las plataformas en cintas magnéticas y en un servidor dedicado. Las pruebas de eficiencia que se realizan han garantizado la recuperación total de la plataforma en un periodo máximo de doce horas. Actualmente no se cuenta con un sitio redundante o alterno.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-02	
Nombre del sistema A1) *	Comunidad PreFA	
Recurso*	Descripción*	Control*
Bitácoras del sistema	Revisión aleatoria del contenido de los logs del sistema operativo y aplicación.	Se realiza una revisión no automatizada buscando patrones de ataque conocidos y secuencias de ataques conocidas como el descubrimiento de puertos y búsqueda de archivos de configuración conocidos.  Responsables: Departamento de Operaciones y Seguridad Informática.

### 7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-02	
Nombre del sistema A1) *	Comunidad PreFA	
Medida de seguridad*	Procedimiento*	Responsable*
Revisión de permisos.	Revisiones de permisos dentro del servidor web y la aplicación.	Responsable: Departamento de Operaciones y Seguridad

		Informática. La duración es de dos horas.
Script de respaldo de información.	Revisión aleatoria del contenido de los respaldos realizados.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización del sistema operativo.	Actualización a nuevas versiones de los paquetes del sistema operativo.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización de la aplicación.	Actualización de framework y librerías de frontend.	Responsable: Coordinación de Bachillerato a distancia.

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-02	
Nombre del sistema A1) *	Comunidad PreFA	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Revisión de permisos.	Se cuentan con los permisos adecuados.	Responsable: Departamento de Operaciones y Seguridad Informática.
Script de respaldos de información.	Los respaldos funcionan correctamente.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización del sistema operativo.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.



Actualización de la aplicación	Actualización de framework y librerías de frontend	Responsable: Coordinación de Bachillerato a distancia
--------------------------------	--	---

#### 7.4. Acciones para la corrección y actualización de las medidas de seguridad


### 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

#### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

No se cuenta con un programa formal de capacitación

#### 8.2. Programa de difusión de la protección a los datos personales (Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

No se tiene un programa de difusión de la protección a los datos personales

### 9. MEJORA CONTINUA

#### 9.1. Actualización y mantenimiento de sistemas de información

Dirección de Bachillerato a Distancia y Mooc			
Identificador único*	CUAIEED-DBDyM-02		
(Nombre del sistema A1) *	Comunidad PreFA		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización de la plataforma a nuevas versiones.	Proceso de actualización hacia versiones superiores del framework Codeigniter y NodeJS.	1 mes.	Total.

## 9.2. Actualización y mantenimiento de equipo de cómputo

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DBDyM-02		
(Nombre del sistema A1*:	Comunidad PreFA		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización del servidor físico.	Cambio del servidor físico utilizado para crear máquinas virtuales donde se hospeda la plataforma.	3 años.	Total.

## 9.3. Procesos para la conservación, preservación y respaldos de información

Dirección de Bachillerato a Distancia y Mooc
--

<b>Identificador único*</b>	CUAIEED-DBDyM-02	
<b>(Nombre del sistema A1*:</b>	<b>Comunidad PreFA</b>	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
<i>Resguardo de cintas magnéticas.</i>	<i>Las cintas magnéticas realizadas en la fase de respaldo automatizado y el lector de las cintas magnéticas son resguardadas de forma indefinida.</i>	<i>Departamento de Operaciones y Seguridad Informática.</i>

#### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

<b>Dirección de Bachillerato a Distancia y Mooc</b>		
<b>Identificador único*</b>	CUAIEED-DBDyM-02	
<b>(Nombre del sistema A1*:</b>	<b>Comunidad PreFA</b>	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
<i>Borrado seguro.</i>	<i>Se realiza un formato de bajo nivel al disco duro físico del hipervisor.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.</i>

### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La Dirección de Bachillerato a Distancia y Mooc recibe o envía la petición en donde se indica la razón para la cancelación del sistema, el tiempo que deberá de permanecer la plataforma funcionando antes de ser eliminada y si se necesita entregar un respaldo final del sistema para su resguardo final en un soporte electrónico. La petición siempre es en formato escrito ya sea por correo electrónico o por oficio. El sistema será eliminado tras una fecha de término establecida y se borra de forma permanente la máquina virtual donde este reside.

## Comunidad Prevet

### Introducción

La plataforma Comunidad Prevet sirve a estudiantes de primer ingreso a la Facultad de Medicina Veterinaria y Zootecnia de la UNAM, así como público en general que tienen interés en fortalecer sus conocimientos base para tener un buen desempeño en su tránsito por el primer año de la licenciatura, al contar con cursos enfocados en temas del área tronco común del área de las ciencias biológicas y de la salud, lectura y redacción y estrategias de aprendizaje en línea. Los usuarios tienen la posibilidad de hacer una prueba inicial por curso para conocer su nivel actual y realizar otra prueba al final del curso para conocer la mejora en su desempeño.

### 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección de Bachillerato a Distancia y Mooc</b>	
<b>Identificador único*</b>	CUAIEED-DBDyM-03
<b>Nombre del sistema A1*:</b>	<b>Comunidad Prevet</b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre, correo electrónico (personal o institucional), género, fecha de nacimiento, escuela de procedencia
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
<b>Nombre*:</b>	Dra. Guadalupe Vadillo Bueno
<b>Cargo*:</b>	Directora de Bachillerato a distancia y MOOC
<b>Funciones*:</b>	Dirección de proyectos educativos de impacto en el programa de Bachillerato a distancia y proyectos externos.
<b>Obligaciones*:</b>	<ul style="list-style-type: none"><li>- Definir junto con los usuarios del sistema, los tipos de acceso.</li><li>- Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.</li></ul>
	<b>Encargados:</b>
<b>(Nombre del Encargado 1*:</b>	Mtro. Alan López de Jesús
<b>Cargo*:</b>	Jefe de Área del Departamento de Operaciones y Seguridad Informática.
<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.

<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 2*:</b>	Mtro. Enrique Tezozomoc Pérez Campos
<b>Cargo*:</b>	Jefe del Departamento de Operaciones y Seguridad Informática
<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 3*:</b>	Mtro. <a href="#">Omar Terrazas Razo</a>
<b>Cargo*:</b>	Coordinador de Bachillerato a distancia
<b>Funciones*:</b>	Coordinador de Bachillerato a distancia y del desarrollo de materiales y sistemas educativos a través de la coordinación del Laboratorio de Arte y Tecnología.
<b>Obligaciones*:</b>	Procurar la protección de los datos personales contenidos en el sistema.
	<b>Usuarios:</b>
<b>(Nombre del Usuario *)</b>	Facultad de Medicina Veterinaria y Zootecnia de la UNAM y público en general.
<b>Cargo*:</b>	Comunidad académica y estudiantil.
<b>Funciones*:</b>	Consultar el contenido de la plataforma, realizar evaluaciones diagnósticas de los cursos que contiene el sitio y evaluaciones para medir su desempeño dentro de la plataforma.
<b>Obligaciones*:</b>	Validar que la información que se distribuye dentro del sistema no contenga datos personales visibles de la comunidad universitaria o un tercero.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

**Dirección de Bachillerato a Distancia y Mooc**

<b>Identificador único*</b>	CUAIEED-DBDyM-03
<b>(Nombre del sistema A1*)</b>	Comunidad Prevet
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos
<b>Características del lugar donde se resguardan los soportes: *</b>	Alojamiento en el centro de datos de CUAIEED dentro de diversas máquinas virtuales, el cual cuenta con acceso mediante un sistema biométrico, planta de energía eléctrica, sistema de respaldo de energía eléctrica ininterrumpida (UPS) y aire acondicionado seco.

### 3. ANÁLISIS DE RIESGOS

Dirección de Bachillerato a Distancia y Moodle		
<b>Identificador único*</b>	CUAIEED-DBDyM-03	
<b>(Nombre del sistema A1) *</b>	Comunidad Prevet	
<b>Riesgo*</b>	<b>Impacto*</b>	<b>Mitigación*</b>
Ingreso no autorizado.	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor.
Explotación de vulnerabilidades.	Medio	Actualización del core del aplicativo desarrollado en PHP Codeigniter.

### 4. ANÁLISIS DE BRECHA

Dirección de Bachillerato a Distancia y Moodle	
<b>Identificador único*</b>	CUAIEED-DBDyM-03

Nombre del sistema A1) *	Comunidad Preve	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Cifrado de comunicaciones entre cliente y servidor.	Uso de certificado de seguridad SSL/TLS en todas las comunicaciones realizadas por la plataforma.	Uso en local de imágenes y librerías javascript empleadas en el frontend.
Actualización de la plataforma.	Trabajar sobre la última versión estable del framework Codeigniter.	Reducir los tiempos requeridos para mantener la plataforma actualizada.

## 5. PLAN DE TRABAJO

Dirección de Bachillerato a Distancia y Mooc			
Identificador único*	CUAIEED-DBDyM-03		
(Nombre del sistema A1) *	Comunidad Preve		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización a la última versión estable del framework	La actualización de la plataforma permite mantener el código fuente en su última versión, con esta actividad se protege la integridad de los datos contenidos en esta.	15 días	Total

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Bachillerato a Distancia y Mooc
--

<b>Identificador único*</b>	CUAIEED-DBDyM-03
<b>(Nombre del sistema A1) *</b>	<b>Comunidad Prevet</b>
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
<b>Transferencias mediante el traslado de soportes físicos:</b>	No se realiza tratamiento de datos personales con soportes físicos, se tiene soporte electrónico en una base de datos.
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias mediante el traslado de soportes electrónicos.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No se realizan transferencias mediante el traslado sobre redes electrónicas.

### **I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

No aplica, se tiene soporte electrónico en una base de datos.

### **II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web y la base de datos de la plataforma, almacenando la fecha, hora, dirección IP, así como todas las acciones dentro del servidor que la aloja. Los archivos de log que se encuentran dentro del sistema operativo se rotan cada diez días mientras que las bitácoras dentro de la base de datos se almacenan de forma indeterminada hasta el final de la vida útil del sistema. La integridad de las bitácoras se garantiza utilizando una suma de HASH. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática, las herramientas utilizadas para el análisis son AWK, SED y GREP.

### **III. REGISTRO DE INCIDENTES**

Los incidentes son reportados al Departamento de Operaciones y Seguridad Informática en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuenta con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

El tipo de soporte es electrónico por lo que la recuperación de la base de datos, la cual se encarga de almacenar los datos personales de los usuarios, es el proceso más importante. Este consiste en recuperar la copia de la base de datos obtenida en el proceso de respaldo programado.

### **V. ACCESO A LAS INSTALACIONES**

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente. La dependencia se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente, se cuenta con un sistema de



videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el director de la Dirección de Desarrollo de Sistemas para la Educación.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

El procedimiento para actualizar o corregir datos personales se encuentra indicado dentro de la plataforma, información disponible únicamente para el usuario registrado, y el cual consiste en entrar a su perfil y actualizar la información de los campos que se encuentran disponibles en el formulario. En el caso de actualización de nombre, correo electrónico o número de cuenta debe solicitarlo vía correo electrónico a la dirección [bunam\\_apps@cuaieed.unam.mx](mailto:bunam_apps@cuaieed.unam.mx).

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

Los perfiles de usuario en esta plataforma únicamente nos permiten separar el tipo de usuario de manera estadística pero no implica algún cambio en los permisos o funciones de la plataforma. El sistema de cuentas de usuario local cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible utilizando MD5.

Existe un tipo de usuario que tiene acceso únicamente a información estadística relacionada con el desempeño de los estudiantes, omitiendo la información de nombre, correo electrónico y número de cuenta. El acceso a estas consultas se realiza desde un sitio independiente que no se encuentra enlazado desde el sitio principal de la plataforma.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

Las plataformas son respaldadas utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello, por un promedio de treinta días tras, y almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas seguras y en condiciones óptimas para su funcionamiento. Para promover la conservación y preservación de la información, las cintas y el lector de estas se mantienen por tiempo indefinido.

## **IX. PLAN DE CONTINGENCIA**

Se cuenta con un plan de contingencia que permite la continuidad de negocio, el cual utiliza como fuente primordial los respaldos obtenidos de las plataformas en cintas magnéticas y en un servidor dedicado. Las pruebas de eficiencia que se realizan han garantizado la recuperación total de la plataforma en un periodo máximo de doce horas. Actualmente no se cuenta con un sitio redundante o alternativo.

## **7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD**

### **7.1. Herramientas y recursos para monitoreo de la protección de datos personales**

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-03	
Nombre del sistema A1) *	Comunidad Prevet	
Recurso*	Descripción*	Control*
Bitácoras del sistema	Revisión aleatoria del contenido de los logs del sistema operativo y aplicación.	Se realiza una revisión no automatizada buscando patrones de ataque conocidos y secuencias de ataques conocidas como el descubrimiento de puertos y búsqueda de archivos de configuración conocidos.  Responsables: Departamento de Operaciones y Seguridad Informática.

## 7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-03	
Nombre del sistema A1) *	Comunidad Prevet	
Medida de seguridad*	Procedimiento*	Responsable*
Revisión de permisos	Revisiones de permisos dentro del servidor web y la aplicación.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de dos horas.

Script de respaldo de información.	Revisión aleatoria del contenido de los respaldos realizados.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización del sistema operativo.	Actualización a nuevas versiones de los paquetes del sistema operativo.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización de la aplicación.	Actualización de framework.	Responsable: Coordinación de Bachillerato a distancia.

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-03	
Nombre del sistema A1) *	Comunidad Prevet	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Revisión de permisos.	Se cuentan con los permisos adecuados.	Responsable: Departamento de Operaciones y Seguridad Informática.
Script de respaldos de información.	Los respaldos funcionan correctamente.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización del sistema operativo.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización de la aplicación.	Actualización de framework.	Responsable: Coordinación de Bachillerato a distancia.

#### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección de Bachillerato a Distancia y Mooc		
Identificador único	CUAIEED-DBDyM-03	
Nombre del sistema A1) *	Comunidad Preve	
Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL	Realizar la renovación anual del certificado SSL	Responsable: Dirección de Desarrollo de Sistemas para la Educación
Actualización de la aplicación	Actualización de framework	Responsable: Coordinación de Bachillerato a distancia

#### 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

##### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

No se cuenta con un programa formal de capacitación

##### 8.2. Programa de difusión de la protección a los datos personales (Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

No se tiene un programa de difusión de la protección a los datos personales

#### 9. MEJORA CONTINUA

##### 9.1. Actualización y mantenimiento de sistemas de información

Dirección de Bachillerato a Distancia y Mooc	
Identificador único*	CUAIEED-DBDyM-03

<b>(Nombre del sistema A1) * Comunidad Prevet</b>			
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
<i>Actualización de la plataforma a nuevas versiones.</i>	<i>Proceso de actualización hacia versiones superiores del framework Codeigniter.</i>	<i>1 mes.</i>	<i>Total.</i>

### 9.2. Actualización y mantenimiento de equipo de cómputo

<b>Dirección de Desarrollo de Sistemas para la Educación</b>			
<b>Identificador único*</b>	CUAIEED-DBDyM-03		
<b>(Nombre del sistema A1*):</b>	<b>Comunidad Prevet</b>		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
<i>Actualización del servidor físico.</i>	<i>Cambio del servidor físico utilizado para crear máquinas virtuales donde se hospeda la plataforma.</i>	<i>3 años.</i>	<i>Total.</i>

### 9.3. Procesos para la conservación, preservación y respaldos de información

<b>Dirección de Bachillerato a Distancia y Mooc</b>	
<b>Identificador único*</b>	CUAIEED-DBDyM-03
<b>(Nombre del sistema A1*):</b>	<b>Comunidad Prevet</b>

Proceso*	Descripción*	Responsable*
Resguardo de cintas magnéticas.	Las cintas magnéticas realizadas en la fase de respaldo automatizado y el lector de las cintas magnéticas son resguardadas de forma indefinida.	Departamento de Operaciones y Seguridad Informática.

#### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-03	
(Nombre del sistema A1*:	Comunidad Prevet	
Proceso*	Descripción*	Responsable*
Borrado seguro.	Se realiza un formato de bajo nivel al disco duro físico del hipervisor.	Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.

### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La Dirección de Bachillerato a Distancia y Mooc recibe o envía la petición en donde se indica la razón para la cancelación del sistema, el tiempo que deberá de permanecer la plataforma funcionando antes de ser eliminada y si se necesita entregar un respaldo final del sistema para su resguardo final en un soporte electrónico. La petición siempre es en formato escrito ya sea por correo electrónico o por oficio. El sistema será eliminado tras una fecha de término establecida y se borra de forma permanente la máquina virtual donde este reside.

#### **Esp BUNAM**

##### **Introducción**

La plataforma Esp BUNAM sirve a estudiantes de B@UNAM, escuelas incorporadas y público en general que tienen interés en fortalecer sus habilidades en el uso correcto de ortografía y signo de puntuación. Los usuarios trabajan a través de una serie de prueba que les propone ejemplos correctos e incorrectos de sentencias en español.

## 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección de Bachillerato a Distancia y Mooc</b>	
<b>Identificador único*</b>	CUAIEED-DBDyM-04
<b>Nombre del sistema A1*:</b>	<b>Esp BUNAM</b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre, correo electrónico (personal o institucional), genero, fecha de nacimiento, escuela de procedencia
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
<b>Nombre*:</b>	Dra. Guadalupe Vadillo Bueno
<b>Cargo*:</b>	Directora de Bachillerato a distancia y MOOC
<b>Funciones*:</b>	Dirección de proyectos educativos de impacto en el programa de Bachillerato a distancia y proyectos externos.
<b>Obligaciones*:</b>	<ul style="list-style-type: none"> <li>- Definir junto con los usuarios del sistema, los tipos de acceso.</li> <li>- Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.</li> </ul>
	<b>Encargados:</b>
<b>(Nombre del Encargado 1*:</b>	Mtro. Alan López de Jesús
<b>Cargo*:</b>	Jefe de Área del Departamento de Operaciones y Seguridad Informática.
<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 2*:</b>	Mtro. Enrique Tezozomoc Pérez Campos
<b>Cargo*:</b>	Jefe del Departamento de Operaciones y Seguridad Informática

<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 3*:</b>	Mtro. <a href="#">Omar Terrazas Razo</a>
<b>Cargo*:</b>	Coordinador de Bachillerato a distancia
<b>Funciones*:</b>	Coordinador de Bachillerato a distancia y del desarrollo de materiales y sistemas educativos a través de la coordinación del Laboratorio de Arte y Tecnología.
<b>Obligaciones*:</b>	Procurar la protección de los datos personales contenidos en el sistema.
	<b>Usuarios:</b>
<b>(Nombre del Usuario *)</b>	Facultad de Medicina Veterinaria y Zootecnia de la UNAM y público en general.
<b>Cargo*:</b>	Comunidad académica y estudiantil.
<b>Funciones*:</b>	Consultar el contenido de la plataforma, realizar evaluaciones diagnósticas de los cursos que contiene el sitio y evaluaciones para medir su desempeño dentro de la plataforma.
<b>Obligaciones*:</b>	Validar que la información que se distribuye dentro del sistema no contenga datos personales visibles de la comunidad universitaria o un tercero.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección de Bachillerato a Distancia y Mooc</b>	
<b>Identificador único*</b>	CUAIEED-DBDyM-04
<b>(Nombre del sistema A1*)</b>	Esp BUNAM
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos



<b>Características del lugar donde se resguardan los soportes: *</b>	Alojamiento en el centro de datos de CUAIEED dentro de diversas máquinas virtuales, el cual cuenta con acceso mediante un sistema biométrico, planta de energía eléctrica, sistema de respaldo de energía eléctrica ininterrumpida (UPS) y aire acondicionado seco.
--	---

### 3. ANÁLISIS DE RIESGOS

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-04	
Nombre del sistema A1) *	Esp BUNAM	
Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado.	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor.
Explotación de vulnerabilidades.	Medio	Actualización del core del aplicativo desarrollado en PHP Codeigniter.

### 4. ANÁLISIS DE BRECHA

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-04	
Nombre del sistema A1) *	Esp BUNAM	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*

Cifrado de comunicaciones entre cliente y servidor.	Uso de certificado de seguridad SSL/TLS en todas las comunicaciones realizadas por la plataforma.	Uso en local de imágenes y librerías javascript empleadas en el frontend.
Actualización de la plataforma.	Trabajar sobre la última versión estable del framework Codeigniter.	Reducir los tiempos requeridos para mantener la plataforma actualizada.

## 5. PLAN DE TRABAJO

Dirección de Bachillerato a Distancia y Mooc			
Identificador único*	CUAIEED-DBDyM-04		
(Nombre del sistema A1) *	Esp BUNAM		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización a la última versión estable del framework	La actualización de la plataforma permite mantener el código fuente en su última versión, con esta actividad se protege la integridad de los datos contenidos en esta.	15 días	Total

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Bachillerato a Distancia y Mooc	
Identificador único*	CUAIEED-DBDyM-04
(Nombre del sistema A1) *	Esp BUNAM

<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
<b>Transferencias mediante el traslado de soportes físicos:</b>	No se realiza tratamiento de datos personales con soportes físicos, se tiene soporte electrónico en una base de datos.
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias mediante el traslado de soportes electrónicos.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No se realizan transferencias mediante el traslado sobre redes electrónicas.

### **I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

No aplica, se tiene soporte electrónico en una base de datos.

### **II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web y la base de datos de la plataforma, almacenando la fecha, hora, dirección IP, así como todas las acciones dentro del servidor que la aloja. Los archivos de log que se encuentran dentro del sistema operativo se rotan cada diez días mientras que las bitácoras dentro de la base de datos se almacenan de forma indeterminada hasta el final de la vida útil del sistema. La integridad de las bitácoras se garantiza utilizando una suma de HASH. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática, las herramientas utilizadas para el análisis son AWK, SED y GREP.

### **III. REGISTRO DE INCIDENTES**

Los incidentes son reportados al Departamento de Operaciones y Seguridad Informática en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuenta con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

El tipo de soporte es electrónico por lo que la recuperación de la base de datos, la cual se encarga de almacenar los datos personales de los usuarios, es el proceso más importante. Este consiste en recuperar la copia de la base de datos obtenida en el proceso de respaldo programado.

### **V. ACCESO A LAS INSTALACIONES**

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente. La dependencia se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el director de la Dirección de Desarrollo de Sistemas para la Educación.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

El procedimiento para actualizar o corregir datos personales se encuentra indicado dentro de la plataforma, información disponible únicamente para el usuario registrado, y el cual consiste en entrar a su perfil y actualizar la información de los campos que se encuentran disponibles en el formulario. En el caso de actualización de nombre, correo electrónico o número de cuenta debe solicitarlo vía correo electrónico a la dirección [bunam\\_apps@cuaieed.unam.mx](mailto:bunam_apps@cuaieed.unam.mx).

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

Los perfiles de usuario en esta plataforma únicamente nos permiten separar el tipo de usuario de manera estadística pero no implica algún cambio en los permisos o funciones de la plataforma. El sistema de cuentas de usuario local cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible utilizando MD5.

Existe un tipo de usuario que tiene acceso únicamente a información estadística relacionada con el desempeño de los estudiantes, omitiendo la información de nombre, correo electrónico y número de cuenta. El acceso a estas consultas se realiza desde un sitio independiente que no se encuentra enlazado desde el sitio principal de la plataforma.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

Las plataformas son respaldadas utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello, por un promedio de treinta días tras, y almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas seguras y en condiciones óptimas para su funcionamiento. Para promover la conservación y preservación de la información, las cintas y el lector de estas se mantienen por tiempo indefinido.

## **IX. PLAN DE CONTINGENCIA**

Se cuenta con un plan de contingencia que permite la continuidad de negocio, el cual utiliza como fuente primordial los respaldos obtenidos de las plataformas en cintas magnéticas y en un servidor dedicado. Las pruebas de eficiencia que se realizan han garantizado la recuperación total de la plataforma en un periodo máximo de doce horas. Actualmente no se cuenta con un sitio redundante o alterno.

## **7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD**

### **7.1. Herramientas y recursos para monitoreo de la protección de datos personales**

Dirección de Bachillerato a Distancia y Moodle	
Identificador único	CUAIEED-DBDVM-04

Nombre del sistema A1) *	Esp BUNAM	
Recurso*	Descripción*	Control*
Bitácoras del sistema	Revisión aleatoria del contenido de los logs del sistema operativo y aplicación.	Se realiza una revisión no automatizada buscando patrones de ataque conocidos y secuencias de ataques conocidas como el descubrimiento de puertos y búsqueda de archivos de configuración conocidos.  Responsables: Departamento de Operaciones y Seguridad Informática.

## 7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-04	
Nombre del sistema A1) *	Esp BUNAM	
Medida de seguridad*	Procedimiento*	Responsable*
Revisión de permisos.	Revisiones de permisos dentro del servidor web y la aplicación.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de dos horas.
Script de respaldo de información.	Revisión aleatoria del contenido de los respaldos realizados.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.

Actualización del sistema operativo.	Actualización a nuevas versiones de los paquetes del sistema operativo.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización de la aplicación.	Actualización de framework.	Responsable: Coordinación de Bachillerato a distancia.

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección de Bachillerato a Distancia y Moodle		
Identificador único*	CUAIEED-DBDyM-04	
Nombre del sistema A1) *	Esp BUNAM	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Revisión de permisos.	Se cuentan con los permisos adecuados.	Responsable: Departamento de Operaciones y Seguridad Informática.
Script de respaldos de información.	Los respaldos funcionan correctamente.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización del sistema operativo.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización de la aplicación.	Actualización de framework.	Responsable: Coordinación de Bachillerato a distancia.

### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-04	
Nombre del sistema A1) *	Esp BUNAM	
Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL.	Realizar la renovación anual del certificado SSL.	Responsable: Dirección de Desarrollo de Sistemas para la Educación.
Actualización de la aplicación.	Actualización de framework.	Responsable: Coordinación de Bachillerato a distancia.

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

No se cuenta con un programa formal de capacitación

### 8.2. Programa de difusión de la protección a los datos personales (Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

No se tiene un programa de difusión de la protección a los datos personales

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

Dirección de Bachillerato a Distancia y Mooc	
Identificador único*	CUAIEED-DBDyM-04

<b>(Nombre del sistema A1) * Esp BUNAM</b>			
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
<i>Actualización de la plataforma a nuevas versiones.</i>	<i>Proceso de actualización hacia versiones superiores del framework Codeigniter.</i>	<i>1 mes.</i>	<i>Total.</i>

### 9.2. Actualización y mantenimiento de equipo de cómputo

<b>Dirección de Desarrollo de Sistemas para la Educación</b>			
<b>Identificador único*</b>	CUAIEED-DBDyM-04		
<b>(Nombre del sistema A1*):</b>	<b>Esp BUNAM</b>		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
<i>Actualización del servidor físico.</i>	<i>Cambio del servidor físico utilizado para crear máquinas virtuales donde se hospeda la plataforma.</i>	<i>3 años.</i>	<i>Total.</i>

### 9.3. Procesos para la conservación, preservación y respaldos de información

<b>Dirección de Bachillerato a Distancia y Mooc</b>	
<b>Identificador único*</b>	CUAIEED-DBDyM-04
<b>(Nombre del sistema A1*):</b>	<b>Esp BUNAM</b>



Proceso*	Descripción*	Responsable*
Resguardo de cintas magnéticas.	Las cintas magnéticas realizadas en la fase de respaldo automatizado y el lector de las cintas magnéticas son resguardadas de forma indefinida.	Departamento de Operaciones y Seguridad Informática.

#### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-04	
(Nombre del sistema A1*:	Esp BUNAM	
Proceso*	Descripción*	Responsable*
Borrado seguro.	Se realiza un formato de bajo nivel al disco duro físico del hipervisor.	Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.

### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La Dirección de Bachillerato a Distancia y Mooc recibe o envía la petición en donde se indica la razón para la cancelación del sistema, el tiempo que deberá de permanecer la plataforma funcionando antes de ser eliminada y si se necesita entregar un respaldo final del sistema para su resguardo final en un soporte electrónico. La petición siempre es en formato escrito ya sea por correo electrónico o por oficio. El sistema será eliminado tras una fecha de término establecida y se borra de forma permanente la máquina virtual donde este reside.

#### **Guía Educativa IME**

##### **Introducción**

La Guía Educativa IME sirve a la diáspora mexicana, principalmente en Estados Unidos brindando información sobre materiales educativos, becas, revalidaciones de estudios, opciones digitales, cursos y carreras técnicas, además de los números telefónicos, correos y direcciones a los que se pueden dirigir para resolver sus dudas relacionadas con trámites y retorno al país. Este es un proyecto desarrollado en

conjunto con el Instituto de los Mexicanos en el Exterior.

## 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección de Bachillerato a Distancia y Mooc</b>	
<b>Identificador único*</b>	CUAIEED-DBDyM-05
<b>Nombre del sistema A1*:</b>	<b>Guía Educativa IME</b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Correo electrónico
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
<b>Nombre*:</b>	Dra. Guadalupe Vadillo Bueno
<b>Cargo*:</b>	Directora de Bachillerato a distancia y MOOC
<b>Funciones*:</b>	Dirección de proyectos educativos de impacto en el programa de Bachillerato a distancia y proyectos externos.
<b>Obligaciones*:</b>	<ul style="list-style-type: none"> <li>- Definir junto con los usuarios del sistema, los tipos de acceso.</li> <li>- Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.</li> </ul>
	<b>Encargados:</b>
<b>(Nombre del Encargado 1*:</b>	Mtro. Alan López de Jesús
<b>Cargo*:</b>	Jefe de Área del Departamento de Operaciones y Seguridad Informática.
<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 2*:</b>	Mtro. Enrique Tezozomoc Pérez Campos
<b>Cargo*:</b>	Jefe del Departamento de Operaciones y Seguridad Informática

<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 3*:</b>	Mtro. Omar Terrazas Razo
<b>Cargo*:</b>	Coordinador de Bachillerato a distancia
<b>Funciones*:</b>	Coordinador de Bachillerato a distancia y del desarrollo de materiales y sistemas educativos a través de la coordinación del Laboratorio de Arte y Tecnología.
<b>Obligaciones*:</b>	Procurar la protección de los datos personales contenidos en el sistema.
	<b>Usuarios:</b>
<b>(Nombre del Usuario *)</b>	Facultad de Medicina Veterinaria y Zootecnia de la UNAM y público en general.
<b>Cargo*:</b>	Comunidad académica y estudiantil.
<b>Funciones*:</b>	Consultar el contenido de la plataforma, realizar evaluaciones diagnósticas de los cursos que contiene el sitio y evaluaciones para medir su desempeño dentro de la plataforma.
<b>Obligaciones*:</b>	Validar que la información que se distribuye dentro del sistema no contenga datos personales visibles de la comunidad universitaria o un tercero.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección de Bachillerato a Distancia y Mooc</b>	
<b>Identificador único*</b>	CUAIEED-DBDyM-05
<b>(Nombre del sistema A1*)</b>	Guía Educativa IME
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos

<b>Características del lugar donde se resguardan los soportes: *</b>	Alojamiento en el centro de datos de CUAIEED dentro de diversas máquinas virtuales, el cual cuenta con acceso mediante un sistema biométrico, planta de energía eléctrica, sistema de respaldo de energía eléctrica ininterrumpida (UPS) y aire acondicionado seco.
--	---

### 3. ANÁLISIS DE RIESGOS

Dirección de Bachillerato a Distancia y Mooc		
<b>Identificador único*</b>	CUAIEED-DBDyM-05	
<b>Nombre del sistema A1) *</b>	<i>Guía Educativa IME</i>	
<b>Riesgo*</b>	<b>Impacto*</b>	<b>Mitigación*</b>
Explotación de vulnerabilidades.	Medio	Actualización de la versión de ReactJS en la que se desarrolló la aplicación.

### 4. ANÁLISIS DE BRECHA

Dirección de Bachillerato a Distancia y Mooc		
<b>Identificador único*</b>	CUAIEED-DBDyM-05	
<b>Nombre del sistema A1) *</b>	<i>Guía Educativa IME</i>	
<b>Medida de seguridad actual*</b>	<b>Medida de seguridad necesaria*</b>	<b>Acciones para remediación*</b>
Cifrado de comunicaciones entre cliente y servidor.	Uso de certificado de seguridad SSL/TLS en todas las comunicaciones realizadas por la plataforma.	Uso en local de imágenes y librerías javascript empleadas en el frontend.

Actualización de la plataforma.	Trabajar sobre la última versión estable del framework ReactJS.	Reducir los tiempos requeridos para mantener la plataforma actualizada.
---------------------------------	---	---

## 5. PLAN DE TRABAJO

Dirección de Bachillerato a Distancia y Mooc			
Identificador único*	CUAIEED-DBDyM-05		
(Nombre del sistema A1) *	Guía Educativa IME		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización a la última versión estable del framework	La actualización de la plataforma permite mantener el código fuente en su última versión, con esta actividad se protege la integridad de los datos contenidos en esta.	15 días	Total

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Bachillerato a Distancia y Mooc	
Identificador único*	CUAIEED-DBDyM-05
(Nombre del sistema A1) *	Guía Educativa IME
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
Transferencias mediante el traslado de soportes físicos:	No se realiza tratamiento de datos personales con soportes físicos, se tiene soporte electrónico en una base de datos.

<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias mediante el traslado de soportes electrónicos.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No se realizan transferencias mediante el traslado sobre redes electrónicas.

## **I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

No aplica, se tiene soporte electrónico en una base de datos.

## **II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web, almacenando la fecha, hora, dirección IP, así como todas las acciones dentro del servidor que la aloja. Los archivos de log que se encuentran dentro del sistema operativo se rotan cada diez días mientras que las bitácoras dentro de la base de datos se almacenan de forma indeterminada hasta el final de la vida útil del sistema. La integridad de las bitácoras se garantiza utilizando una suma de HASH. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática, las herramientas utilizadas para el análisis son AWK, SED y GREP.

## **III. REGISTRO DE INCIDENTES**

Los incidentes son reportados al Departamento de Operaciones y Seguridad Informática en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuenta con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

## **V. ACCESO A LAS INSTALACIONES**

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente. La dependencia se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el director de la Dirección de Desarrollo de Sistemas para la Educación.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

No existe un procedimiento de actualización de datos personales, la sesión de usuario es manejada a través de Oauth 2.0 y almacenado el correo electrónico en una base de datos Google Firebase en la que se registra el correo electrónico y la fecha de registro.

## VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los perfiles de usuario en esta plataforma únicamente nos permiten separar el tipo de usuario de manera estadística pero no implica algún cambio en los permisos o funciones de la plataforma. El registro del usuario por medio de correo electrónico únicamente es usado con fines estadísticos de uso de la Guía Educativa.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Las plataformas son respaldadas utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello, por un promedio de treinta días tras, y almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas seguras y en condiciones óptimas para su funcionamiento. Para promover la conservación y preservación de la información, las cintas y el lector de estas se mantienen por tiempo indefinido.

## IX. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de negocio, el cual utiliza como fuente primordial los respaldos obtenidos de las plataformas en cintas magnéticas y en un servidor dedicado. Las pruebas de eficiencia que se realizan han garantizado la recuperación total de la plataforma en un periodo máximo de doce horas. Actualmente no se cuenta con un sitio redundante o alterno.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-05	
(Nombre del sistema A1) *	Guía Educativa IME	
Recurso*	Descripción*	Control*
Bitácoras del sistema	Revisión aleatoria del contenido de los logs del sistema operativo y aplicación.	Se realiza una revisión no automatizada buscando patrones de ataque conocidos y secuencias de ataques conocidas como el descubrimiento de puertos y búsqueda de archivos de configuración conocidos.

		Responsables: Departamento de Operaciones y Seguridad Informática.
--	--	--

### 7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-05	
Nombre del sistema A1) *	Guía Educativa IME	
Medida de seguridad*	Procedimiento*	Responsable*
Revisión de permisos.	Revisiones de permisos dentro del servidor web y la aplicación.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de dos horas.
Script de respaldo de información.	Revisión aleatoria del contenido de los respaldos realizados.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización del sistema operativo.	Actualización a nuevas versiones de los paquetes del sistema operativo.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización de la aplicación.	Actualización de framework.	Responsable: Coordinación de Bachillerato a distancia.

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección de Bachillerato a Distancia y Mooc		
--	--	--



<b>Dirección de Bachillerato a Distancia y Mooc</b>		
<b>Identificador único*</b>	CUAIEED-DBDyM-05	
<b>Nombre del sistema A1) *</b>	Guía Educativa IME	
<b>Medida de seguridad*</b>	<b>Resultado de evaluación*</b>	<b>Responsable*</b>
Revisión de permisos.	Se cuentan con los permisos adecuados.	Responsable: Departamento de Operaciones y Seguridad Informática.
Script de respaldos de información.	Los respaldos funcionan correctamente.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización del sistema operativo.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización de la aplicación.	Actualización de framework.	Responsable: Coordinación de Bachillerato a distancia.

#### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

<b>Dirección de Bachillerato a Distancia y Mooc</b>		
<b>Identificador único*</b>	CUAIEED-DBDyM-05	
<b>Nombre del sistema A1) *</b>	Guía Educativa IME	
<b>Medida de seguridad*</b>	<b>Acciones*</b>	<b>Responsable*</b>
Uso de certificados SSL.	Realizar la renovación anual del certificado SSL.	Responsable: Dirección de Desarrollo de Sistemas para la Educación.

Actualización de la aplicación

Actualización de framework

Responsable: Coordinación de Bachillerato a distancia

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

No se cuenta con un programa formal de capacitación

### 8.2. Programa de difusión de la protección a los datos personales

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

No se tiene un programa de difusión de la protección a los datos personales

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

Dirección de Bachillerato a Distancia y Mooc			
Identificador único*	CUAIEED-DBDyM-05		
(Nombre del sistema A1) *	Guía Educativa IME		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización de la plataforma a nuevas versiones.	Proceso de actualización hacia versiones superiores del framework ReactJS.	1 mes.	Total.

### 9.2. Actualización y mantenimiento de equipo de cómputo

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DBDyM-05		
(Nombre del sistema A1*:	Guía Educativa IME		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización del servidor físico.	<i>Cambio del servidor físico utilizado para crear máquinas virtuales donde se hospeda la plataforma.</i>	3 años.	Total.

### 9.3. Procesos para la conservación, preservación y respaldos de información

Dirección de Bachillerato a Distancia y Mooc		
Identificador único*	CUAIEED-DBDyM-05	
(Nombre del sistema A1*:	Guía Educativa IME	
Proceso*	Descripción*	Responsable*
Resguardo de cintas magnéticas.	<i>Las cintas magnéticas realizadas en la fase de respaldo automatizado y el lector de las cintas magnéticas son resguardadas de forma indefinida.</i>	<i>Departamento de Operaciones y Seguridad Informática.</i>

### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección de Bachillerato a Distancia y Mooc
--

<b>Identificador único*</b>	CUAIEED-DBDyM-05	
<b>(Nombre del sistema A1*:</b>	Guía Educativa IME	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
<i>Borrado seguro.</i>	<i>Se realiza un formato de bajo nivel al disco duro físico del hipervisor.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.</i>

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La Dirección de Bachillerato a Distancia y Mooc recibe o envía la petición en donde se indica la razón para la cancelación del sistema, el tiempo que deberá de permanecer la plataforma funcionando antes de ser eliminada y si se necesita entregar un respaldo final del sistema para su resguardo final en un soporte electrónico. La petición siempre es en formato escrito ya sea por correo electrónico o por oficio. El sistema será eliminado tras una fecha de término establecida y se borra de forma permanente la máquina virtual donde este reside.

### Sistema de gestión de constancias (SIGECO)

#### Introducción

El Sistema de Gestión Constancias (SIGECO) se desarrolló como una herramienta de transformación digital para atender las necesidades de los usuarios de Educación Continua de la Universidad bajo las premisas de ahorro anual en impresiones, eficiencia en el registro oficial de cada constancia emitida usando la Firma Electrónica Universitaria (FEU) de la UNAM, así como la seguridad informática durante el proceso, emisión y entrega de constancias generadas. El sistema opera con dos perfiles: el Administrador y el Firmante. Necesariamente, se requiere una cuenta de correo electrónico institucional para el seguimiento de entrega y envío de las constancias emitidas.

El SIGECO es un sistema 100% en línea que se encuentra alojado en los servidores de la CUAIEED en la dirección electrónica: <https://sigeco.cuaieed.unam.mx/>. Para ingresar al sistema y hacer uso del SIGECO, la Dirección de Desarrollo de Sistemas para la Educación (DDSE) asigna una cuenta de administrador y cuentas para los firmantes de la Coordinación.

En SIGECO se pueden emitir constancias con un máximo de cuatro firmas y se recomienda que los firmantes cuenten con la FEU-UNAM; en caso contrario, se deberá requisitar un formato especial que incorpore al menos una FEU, más la(s) firmas autógrafas de quien(es) aparecerá(n) como firmante(s) de la constancia. Para la emisión de una constancia es indispensable contar con la CURP, nombre completo y correo electrónico de la persona a quien se le emitirá. Para el caso de participantes extranjeros, se puede utilizar el Código de identidad, o ID o la CURP para extranjeros que proporciona la Secretaría de Relaciones Exteriores.

## 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

**Dirección de Desarrollo de Sistemas para la Educación**

<b>Identificador único*</b>	CUAIEED-DDSE-01
<b>(Nombre del sistema) *</b>	<b>Sistema de Gestión de Constancias (SIGECO)</b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre, apellidos, calificaciones, CURP, RFC, código de identidad, correo electrónico, fecha de nacimiento, género, nacionalidad, nivel académico, entidad o facultad a la que pertenece
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
<b>Nombre*:</b>	Mtro. Ricardo Arroyo Mendoza
<b>Cargo*:</b>	Director de la Dirección de Desarrollo de Sistemas para la Educación.
<b>Funciones*:</b>	Definir la arquitectura tecnológica necesaria para el funcionamiento y mantenimiento del sistema.
<b>Obligaciones*:</b>	<ul style="list-style-type: none"> <li>• Autorizar la creación de los usuarios con accesos administrativos al sistema, solicitados por las entidades y dependencias universitarias.</li> <li>• Vigilar que el sistema cumpla con todas las medidas de seguridad técnica, físicas y administrativas.</li> </ul>
	<b>Encargados<sup>1</sup>:</b>
<b>(Nombre del Encargado 1*)</b>	<b>Mtro. Eduardo López Molina</b>
<b>Cargo*:</b>	<b>Coordinador de Informática y Proyectos de Tecnologías de la Información</b>
<b>Funciones*:</b>	<ul style="list-style-type: none"> <li>• Desarrollador de sistemas para la educación.</li> <li>• Creación, Mejora continua, actualización, mantenimiento preventivo y correctivo de los sistemas de la Dirección de Desarrollo de Sistemas para la Educación.</li> </ul>
<b>Obligaciones*:</b>	Cumplir con la confidencialidad de los datos personales.

<sup>1</sup> Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.

	<b>Usuarios:</b>
<b>(Nombre del Usuario 1*)</b>	Irene Anaís Pereda Aguado
<b>Cargo*:</b>	Unidad de Planeación y Vinculación CUAIEED
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 2*)</b>	Daniela Michelle Kury
<b>Cargo*:</b>	Responsable Operativa de la Facultad de Arquitectura
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 3*)</b>	Javier Sacristán
<b>Cargo*:</b>	Educación Continua del PUEAA
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 4*)</b>	Jorge Hernández
<b>Cargo*:</b>	Secretario de Educación Continua Facultad de Medicina, Veterinaria y Zootecnia
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 5*)</b>	Armando Martínez

<b>Cargo*:</b>	Jefe del Departamento de Operación FES Iztacala
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 6*)</b>	Gustavo López
<b>Cargo*:</b>	Coordinador del Instituto Investigaciones Económicas
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 7*)</b>	Daniel Ociel Martínez
<b>Cargo*:</b>	Coordinador Administrativo Facultad de Derecho
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 8*)</b>	Nidia Cendejas
<b>Cargo*:</b>	Jefa del Departamento de desarrollo y operación de TIC DGTIC
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 9*)</b>	Luis Antonio
<b>Cargo*:</b>	Secretario de Enseñanza Instituto de Investigaciones Biomédicas
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO

<b>(Nombre del Usuario 10*)</b>	Miriam Esther Olguin
<b>Cargo*:</b>	Técnico Académico Centro de Investigaciones Sobre América del Norte
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 11*)</b>	Guillermo Chávez
<b>Cargo*:</b>	Subdirector de Revistas Académicas y Publicaciones Dirección General de Publicaciones y Fomento Editorial
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 12*)</b>	Mario Alviso Becerril
<b>Cargo*:</b>	Coordinador de Educación Continua Facultad de Música
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 13*)</b>	Lucila M. Cortina
<b>Cargo*:</b>	Coordinadora de Educación Continua Instituto de Geofísica
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 14*)</b>	Oralia Palos
<b>Cargo*:</b>	Jefa del Dpto. de Extensión Académica Escuela Nacional de



	Artes Cinematográficas
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 15*)</b>	Rafael Sandoval
<b>Cargo*:</b>	Jefe de departamento Facultad de Ingeniería
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 16*)</b>	José Alfredo Delgado
<b>Cargo*:</b>	Coordinador de Redes
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 17*)</b>	Martha Rico
<b>Cargo*:</b>	Coordinadora de Servicios de Cómputo Facultad de Ciencias
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 18*)</b>	Fabiola Villela
<b>Cargo*:</b>	Jefa de Educación Continua ENES Mérida
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO

<b>(Nombre del Usuario 19*)</b>	Liber Iván León
<b>Cargo*:</b>	Secretario Técnico Coordinación General de Posgrado
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 20*)</b>	Susana Lara
<b>Cargo*:</b>	Jefa de la División de Educación Continua Facultad de Psicología
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 21*)</b>	David Ruiz
<b>Cargo*:</b>	Secretario Técnico CEM Sudáfrica
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 22*)</b>	Mariana Sánchez
<b>Cargo*:</b>	Secretaria Técnica de Proyectos del PUEC
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 23*)</b>	Guillermo Gómez
<b>Cargo*:</b>	Jefe del Departamento de Difusión Cultural y Educación Continua de IIBI
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su

	facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 24*)</b>	Erika Liliana López
<b>Cargo*:</b>	Jefa del Departamento de Apoyo a la Docencia, Educación Continua y Diplomados Centro de Investigaciones Interdisciplinarias de Ciencias y Humanidades
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 25*)</b>	Michelle Cardozo
<b>Cargo*:</b>	Jefe Área de educación continua Unidad de Investigación sobre Representaciones Culturales y Sociales
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 26*)</b>	Celeste Morales
<b>Cargo*:</b>	Coordinadora de la Unidad de Educación Continua Instituto de Energías Renovables
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 27*)</b>	Rafael Basilio
<b>Cargo*:</b>	Responsable técnico Dirección General Escuela Nacional Preparatoria
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO

<b>(Nombre del Usuario 28*)</b>	Sandra Roan
<b>Cargo*:</b>	Responsable técnico Unidad Académica de Estudios Regionales
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 29*)</b>	Diana Carina Monterrosa
<b>Cargo*:</b>	Responsable de Educación Continua de la DGDC
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 30*)</b>	Diego Hernández
<b>Cargo*:</b>	Responsable técnico Escuela Nacional Preparatoria Plantel 2
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 31*)</b>	José Alfredo Noriega
<b>Cargo*:</b>	Desarrollo de Software, ENES Morelia
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 32*)</b>	María Aurora García
<b>Cargo*:</b>	Jefa de División ENEO

<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 33*)</b>	Mayela Lara
<b>Cargo*:</b>	Coordinadora de Gestión Coordinación para la Igualdad de Género (CIGU)
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 34*)</b>	María Reyna Ramos
<b>Cargo*:</b>	Coordinadora de Gestión Escuela Nacional de Trabajo Social
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 35*)</b>	Ana Pérez Arteaga
<b>Cargo*:</b>	Secretaría Técnica Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 36*)</b>	Angélica Cruz
<b>Cargo*:</b>	Responsable técnica CEMRU
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 37*)</b>	Juan Mario Pérez

<b>Cargo*:</b>	Secretario Técnico Programa Universitario de Estudios de la Diversidad Cultural y la Interculturalidad
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 38*)</b>	Rocío De La Torre
<b>Cargo*:</b>	Profesora Titular A Instituto de Investigación de Materiales
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 39*)</b>	Irene Vázquez
<b>Cargo*:</b>	Comunicación e Imagen COORDINACIÓN UNIVERSITARIA PARA LA SUSTENTABILIDAD
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 40*)</b>	Andrea Montiel
<b>Cargo*:</b>	Asistente de Dirección ENES Juriquillas
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 41*)</b>	Rossana Gutiérrez
<b>Cargo*:</b>	Departamento de Docencia Centro Regional de Investigaciones Multidisciplinarias
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO

<b>(Nombre del Usuario 42*)</b>	Elsy Patricia Ayllón
<b>Cargo*:</b>	Coordinadora de Gestión Facultad de Ciencias Políticas y Sociales
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 43*)</b>	Gustavo Carreon
<b>Cargo*:</b>	Técnico Académico Programa Universitario de Estudios sobre Educación Superior
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 44*)</b>	Ada Ligia Torres
<b>Cargo*:</b>	Secretaria Técnica Instituto de Investigaciones Antropológicas
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 45*)</b>	Mariana Domínguez
<b>Cargo*:</b>	Jefa del departamento de vinculación Dirección General de Actividades Cinematográficas Filмотeca
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 46*)</b>	Fabiola Villela
<b>Cargo*:</b>	Secretaria técnica, responsable de Educación continua Dirección General de Divulgación de las Humanidades

<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 46*)</b>	Armando Rodríguez
<b>Cargo*:</b>	Secretario de Informática Colegio de Ciencias y Humanidades
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO
<b>(Nombre del Usuario 47*)</b>	Ana Laura Correa Benitez
<b>Cargo*:</b>	Secretario de Informática Centro de Investigaciones sobre América Latina y el Caribe
<b>Funciones*:</b>	Creación, envío y seguimiento de constancias digitales de su facultad/entidad correspondiente por medio del SIGECO
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos en su alta al SIGECO

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

*(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)*

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único**</b>	<i>CUAIEED-DDSE-01</i>
<b>(Nombre del sistema *)</b>	<b>Sistema de Gestión de Constancias (SIGECO)</b>
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos
<b>Características del lugar donde se resguardan los soportes: *</b>	Almacenamiento en el centro de datos de CUAIEED dentro de diversas máquinas virtuales, el cual cuenta con acceso mediante un sistema biométrico, planta de energía eléctrica, sistema de respaldo de energía eléctrica ininterrumpida (UPS) y aire acondicionado seco.

## 3. ANÁLISIS DE RIESGOS



(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-01	
Nombre del sistema) *	Sistema de Gestión de Constancias (SIGECO)	
Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado.	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor.
Explotación de vulnerabilidades.	Medio	Actualización de librerías y frameworks.

#### 4. ANÁLISIS DE BRECHA

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-01	
Nombre del sistema) *	Sistema de Gestión de Constancias (SIGECO)	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Las contraseñas no tienen longitud mínima.	Las contraseñas deben tener una longitud mínima de 8 caracteres.	Se debe actualizar las contraseñas ya existentes y a su vez, agregar a los nuevos usuarios con contraseñas que

		cumplan el requisito mínimo de longitud
Contraseñas seguras de usuario	Las contraseñas de usuario deben ser únicas y rotadas constantemente para evitar el descubrimiento por medio de ataques de diccionario.	Cambio de contraseñas de usuario cada seis meses.
Cifrado de comunicaciones entre cliente y servidor	Uso de certificado de seguridad SSL/TLS en todas las comunicaciones realizadas por el desarrollo.	Uso en local de imágenes y scripts de javascript para la vista web.

## 5. PLAN DE TRABAJO

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-01		
(Nombre del sistema) *	Sistema de Gestión de Constancias (SIGECO)		
Actividad*	Descripción*	Duración*	Cobertura*
Mantenimiento preventivo	Revisión y actualización de código para nuevas versiones compatible con servidor y navegadores	20 horas Semestral	Los datos se encuentran con la seguridad adecuada para no ser consultados por un usuario no autenticado en el sistema

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

**Dirección de Desarrollo de Sistemas para la Educación**

<b>Identificador único*</b>	CUAIEED-DDSE-01
<b>(Nombre del sistema) *</b>	<b>Sistema de Gestión de Constancias (SIGECO)</b>
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
<b>Transferencias mediante el traslado de soportes físicos:</b>	No se realizan transferencias de datos personales mediante el traslado de soportes físicos
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No se realizan transferencias de datos personales mediante el traslado de redes electrónicas.

**I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

No aplica, se tiene soporte electrónico en una base de datos.

**II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web, almacenando la fecha, hora, dirección IP, así como todas las acciones dentro del sistema. Los archivos de log que se encuentran dentro del sistema operativo se rotan cada diez días mientras que las bitácoras dentro de la base de datos se almacenan de forma indeterminada hasta el final de la vida útil del sistema. La integridad de las bitácoras se garantiza utilizando una suma de HASH. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática de la CUAIEED y las herramientas utilizadas para el análisis son AWK, SED y GREP.

**III. REGISTRO DE INCIDENTES**

Los incidentes son reportados al Departamento de Operaciones y Seguridad Informática de la CUAIEED en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuentan con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

El tipo de soporte es electrónico por lo que la recuperación de la base de datos, la cual se encarga de almacenar los datos personales de los usuarios, es el proceso más importante. Este consiste en recuperar el código del desarrollo junto con una copia de la base de datos obtenida en el proceso de respaldo programado.

Tras realizar la recuperación de los datos se realiza una comparación con un respaldo de la base de

datos antes de ser comprometida para validar su estado y determinar la pertinencia de su uso. Si fue utilizado un respaldo para la recuperación se valida su integridad con una suma de HASH.

## **V. ACCESO A LAS INSTALACIONES**

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7, en todas las instalaciones de la dependencia. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, la cual se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias. Las personas que acceden a laborar a las instalaciones se identifican con una identificación oficial vigente.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el director de la Dirección de Desarrollo de Sistemas para la Educación.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

El solicitante de una corrección de datos personales deberá de enviar un ticket a la mesa de ayuda correspondiente del sistema, tras identificarse como usuario, indicando el dato incorrecto seguido de los nuevos datos a actualizar. El cambio se realizará en un plazo no mayor a cuarenta y ocho horas tras ser recibida la solicitud.

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

El modelo de control de acceso al sistema se encuentra basado en roles (perfiles). El sistema operativo donde se hospedan las aplicaciones utiliza un sistema de cuentas de usuario local que cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible. Los nuevos usuarios son creados a partir de un registro por parte del administrador del sistema. Los usuarios trabajan con el sistema mediante una vista web por lo que no requieren de acceso al sistema operativo donde vive la aplicación.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

El sistema es respaldado utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello por un promedio de treinta días, tras lo cual, es almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello, que mantiene las cintas en condiciones óptimas para su funcionamiento. El resguardo de las cintas magnéticas es indefinido.

## **IX. PLAN DE CONTINGENCIA**

Se cuenta con un plan de contingencia que permite la continuidad de la operación, el cual utiliza como fuente primordial los respaldos obtenidos del sistema en cintas magnéticas y en un servidor dedicado. En las pruebas de eficiencia que se realizan, se ha garantizado la recuperación total del

sistema en un periodo máximo de doce horas. Actualmente, no se cuenta con un sitio redundante o alternativo.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

**7.1. Herramientas y recursos para monitoreo de la protección de datos personales**  
*(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)*

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-01	
Nombre del sistema)*	Sistema de Gestión de Constancias (SIGECO)	
Recurso*	Descripción*	Control*
Bitácoras del sistema	Revisión aleatoria del contenido de los logs del sistema operativo y aplicación.	Se realiza una revisión no automatizada buscando patrones de ataque conocidos y secuencias de ataques conocidas como el descubrimiento de puertos y búsqueda de archivos de configuración conocidos.  Responsables: Departamento de Operaciones y Seguridad Informática.

**7.2. Procedimiento para la revisión de las medidas de seguridad**  
*(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)*

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-01
Nombre del sistema)*	Sistema de Gestión de Constancias (SIGECO)

Medida de seguridad*	Procedimiento*	Responsable*
Revisión de permisos.	Revisiones de permisos dentro del servidor web y la aplicación.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de dos horas.
Scripts de respaldos de información.	Revisión aleatoria del contenido de los respaldos realizados.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización del sistema operativo.	Actualización a nuevas versiones de los paquetes del sistema operativo.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización de la aplicación.	Actualización de librerías y frameworks principales del sistema.	Responsable: Coordinador de Informática y Proyectos de Tecnologías de la Información.  Duración es de 20 horas.

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-01	
Nombre del sistema) *	Sistema de Gestión de Constancias (SIGECO)	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Revisión de permisos.	Se cuentan con los permisos adecuados.	Responsable: Departamento de Operaciones y Seguridad Informática.

Scripts de respaldos de información.	Los respaldos funcionan correctamente.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización del sistema operativo.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización de la aplicación.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.

**7.4. Acciones para la corrección y actualización de las medidas de seguridad**  
(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

<b>Dirección de Desarrollo de Sistemas para la Educación</b>		
<b>Identificador único*</b>	CUAIEED-DDSE-01	
<b>Nombre del sistema) *</b>	Sistema de Gestión de Constancias (SIGECO)	
<b>Medida de seguridad*</b>	<b>Acciones*</b>	<b>Responsable*</b>
Uso de certificados SSL.	Realizar la renovación anual del certificado SSL.	Responsable: Dirección de Desarrollo de Sistemas para la Educación.

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

**8.1. Programa de capacitación a los responsables de seguridad de datos personales**  
(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

<b>Dirección de Desarrollo de Sistemas para la Educación</b>
--

<b>Identificador único*</b>	CUAIEED-DDSE-01		
<b>(Nombre del sistema) *</b>	<b>Sistema de Gestión de Constancias (SIGECO)</b>		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Inicio: 19 de abril 2021 Término: 23 de mayo de 2021	Responsables de TI de las dependencias de la UNAM.

## 8.2. Programa de difusión de la protección a los datos personales

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

No se cuenta con un programa de difusión de la protección a los datos personales

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

<b>Dirección de Desarrollo de Sistemas para la Educación</b>			
<b>Identificador único*</b>	CUAIEED-DDSE-01		
<b>(Nombre del sistema) *</b>	<b>Sistema de Gestión de Constancias (SIGECO)</b>		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
Creación de nuevos subsistemas/módulos	<i>Desarrollo WEB para cumplir las nuevas necesidades del usuario, las cuales van surgiendo durante el uso de este.</i>	50 horas cada 3 meses	<i>Creación de reportes Automatización de procesos</i>



### 9.2. Actualización y mantenimiento de equipo de cómputo

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-01		
(Nombre del sistema) *	Sistema de Gestión de Constancias (SIGECO)		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización del servidor físico.	<i>Cambio del servidor físico utilizado para crear máquinas virtuales donde se aloja el sistema.</i>	3 años.	Total.

### 9.3. Procesos para la conservación, preservación y respaldos de información

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-01	
(Nombre del sistema) *	Sistema de Gestión de Constancias (SIGECO)	
Proceso*	Descripción*	Responsable*
Resguardo de cintas magnéticas.	<i>Las cintas magnéticas realizadas en la fase de respaldo automatizado son resguardadas de forma indefinida en un almacén.</i>	<i>Departamento de Operaciones y Seguridad Informática.</i>

**9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos**  
*(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)*

Dirección de Desarrollo de Sistemas para la Educación		
<b>Identificador único*</b>	CUAIEED-DDSE-01	
<b>(Nombre del sistema) *</b>	Sistema de Gestión de Constancias (SIGECO)	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
<i>Borrado seguro.</i>	<i>Se realiza un formato de bajo nivel al disco duro físico del hipervisor.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.</i>

**Encuestas CUAIEED - LimeSurvey**

**Introducción**

LimeSurvey es una aplicación de software libre para la realización de encuestas en línea, escrita en PHP y que utiliza bases de datos MySQL, PostgreSQL o MSSQL. Esta utilidad brinda la posibilidad, a usuarios sin conocimientos de programación, de desarrollar, publicar y recolectar respuestas de sus encuestas. La CUAIEED implementó esta aplicación en los servidores de la UNAM como un servicio para la comunidad.

Las encuestas incluyen ramificación a partir de condiciones, plantillas y diseño personalizado usando un sistema de plantillas web, y provee utilidades básicas de análisis estadístico para el tratamiento de los resultados obtenidos.

Las encuestas pueden tener tanto un acceso público como un acceso controlado por las claves que pueden ser utilizadas una sola vez (tokens) asignadas a cada persona que participa en la encuesta. Además, los resultados pueden ser anónimos, separando los datos de los participantes de los datos que proporcionan, inclusive en encuestas controladas.

**1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES**

Dirección de Desarrollo de Sistemas para la Educación	
<b>Identificador único*</b>	CUAIEED-DDSE-02
<b>(Nombre del sistema A2) *</b>	<b>Encuestas CUAIEED - Limesurvey</b>

<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, costumbres, idioma o lengua, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, trayectoria educativa, certificados y reconocimientos, opiniones políticas, origen racial o étnico, creencias religiosas, creencias filosóficas y morales, afiliación sindical.
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED)
<b>Nombre*:</b>	Mtro. Ricardo Arroyo Mendoza
<b>Cargo*:</b>	Dirección de Desarrollo de Sistemas para la Educación
<b>Funciones*:</b>	Definir la arquitectura tecnológica necesaria para el funcionamiento de la plataforma de encuestas.
<b>Obligaciones*:</b>	Decidir los usuarios y encargados que tendrán accesos administrativos de la plataforma. Vigilar que el sistema cumpla con las medidas de seguridad técnica, físicas y administrativas.
	<b>Encargados:</b>
<b>(Nombre del Encargado 1*)</b>	Mtro. Eduardo López Molina
<b>Cargo*:</b>	Coordinador de Informática y Proyectos de Tecnologías de la Información
<b>Funciones*:</b>	Gestión de acceso, planificación, actualización, seguridad y operación continua del sistema y los datos almacenados
<b>Obligaciones*:</b>	Cuidado de los datos personales Conservación de los datos personales Aseguramiento de los datos personales
	<b>Usuarios:</b>
<b>(Nombre del Usuario 1*)</b>	Encargado de TI de la Escuela, Facultad, Entidad o Coordinación que solicita el acceso
<b>Cargo*:</b>	Encargado de TI
<b>Funciones*:</b>	Decidir qué datos personales se solicitan a los usuarios Decidir cuánto tiempo se mantienen los datos personales en

	el sistema Actualización de los datos dentro del sistema
<b>Obligaciones*:</b>	Cuidado de los datos personales Conservación de los datos personales Aseguramiento de los datos personales

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único*</b>	CUAIEED-DDSE-02
<b>(Nombre del sistema *)</b>	Encuestas CUAIEED - Limesurvey
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Sistema de creación de encuestas
<b>Características del lugar donde se resguardan los soportes: *</b>	Alojamiento en el centro de datos de CUAIEED dentro de diversas máquinas virtuales. El centro de datos cuenta con temperatura controlada y acceso mediante un sistema biométrico.

## 3. ANÁLISIS DE RIESGOS

<b>Dirección de Desarrollo de Sistemas para la Educación</b>		
<b>Identificador único*</b>	CUAIEED-DDSE-02	
<b>(Nombre del sistema A2) *</b>	Encuestas CUAIEED - Limesurvey	
<b>Riesgo*</b>	<b>Impacto*</b>	<b>Mitigación*</b>
Ingreso no autorizado.	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor.
Explotación de vulnerabilidades.	Medio	Actualización del core de la plataforma Limesurvey

Modificación, compartición o robo de información por parte de los usuarios del sistema de encuestas	Alto	Hacer firmar un contrato de confidencialidad a los usuarios sobre el uso de datos personales
---	------	--

#### 4. ANÁLISIS DE BRECHA

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-02	
Nombre del sistema) *	Encuestas CUAIEED - Limesurvey	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Cifrado de comunicaciones entre cliente y servidor.	Uso de certificado de seguridad SSL/TLS en todas las comunicaciones realizadas por la plataforma.	Uso en local de imágenes y scripts de javascript para la vista web.
Contraseñas seguras de usuario.	Las contraseñas de usuario deben ser únicas y rotadas constantemente para evitar el descubrimiento por medio de ataques de diccionario.	Cambio de contraseñas de usuario cada seis meses.
Actualización de la plataforma.	Tras liberarse la actualización de la plataforma Limesurvey se deben de implementar estos cambios inmediatamente.	Reducir los tiempos requeridos para mantener la plataforma actualizada.

#### 5. PLAN DE TRABAJO

Dirección de Desarrollo de Sistemas para la Educación
---

Identificador único*	CUAIEED-DDSE-02		
(Nombre del sistema) *	Encuestas CUAIEED - Limesurvey		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización e instalación de parches de seguridad de la plataforma LimeSurvey	Actualizar la plataforma LimeSurvey en su versión estable y con los parches de seguridad	2 horas	Total
Bitácoras de control de roles	Realizar una bitácora con los nombres de usuarios que ingresan a las plataformas con perfil de usuario	20 horas	Total

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-02
(Nombre del sistema) *	Encuestas CUAIEED - Limesurvey
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
Transferencias mediante el traslado de soportes físicos:	No se realiza el traslado de soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realiza el traslado de soportes electrónicos

<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No se realiza el traslado sobre redes electrónicas
--	--

## **II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

La plataforma de LimeSurvey no realiza tratamiento de datos personales con soporte físico

## **III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Las bitácoras de la plataforma de encuestas LimeSurvey se almacenan en dos lugares:

Una dentro del servidor, en formato de log, y otra dentro del propio sistema que contiene un sistema de bitácoras, en ambas bitácoras se almacena el nombre de usuario, correo electrónico e IP desde donde se conectan los usuarios. Los archivos de log que se encuentran dentro del sistema operativo se rotan cada diez días, mientras que las bitácoras del propio sistema se almacenan de forma indeterminada hasta el final de la vida útil del sistema. La integridad de las bitácoras se garantiza utilizando una suma de HASH. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática de la CUAIEED y las herramientas utilizadas para el análisis son AWK, SED y GREP. Solo los responsables y usuarios con privilegios de administrador pueden ingresar a revisar las bitácoras, en caso de que llegue alguna alerta sobre un inicio de sesión no autorizado y alguna incidencia que requiera la revisión de las bitácoras.

## **IV. REGISTRO DE INCIDENTES:**

Para la plataforma LimeSurvey, los incidentes son reportados al Departamento de Operaciones y Seguridad Informática en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuenta con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

El tipo de soporte es electrónico por lo que la recuperación de la base de datos, la cual se encarga de almacenar los datos personales de los usuarios, es el proceso más importante. Este consiste en recuperar el código fuente del sistema de LimeSurvey junto con una copia de la base de datos obtenida en el proceso de respaldo programado.

Tras realizar la recuperación de los datos se realiza una comparación con un respaldo de la base de datos antes de ser comprometida para validar su estado y determinar la pertinencia de su uso. Si fue utilizado un respaldo para la recuperación, se valida su integridad con una suma de HASH. La recuperación de datos es autorizada por el director de la Dirección de Desarrollo de Sistemas para la Educación.

El incidente se registra en un documento en el cual se da a conocer la siguiente información:

- Nombre del o las personas que registraron el incidente
- Nombre del o las personas que soluciona el incidente
- Daño causado al sistema
- Acciones realizadas para asegurar la integridad de los datos
- Tiempo de recuperación de la incidencia
- Medidas para evitar el incidente a futuro

## **V. ACCESO A LAS INSTALACIONES**



El acceso a la coordinación es a través de la caseta de control en la entrada principal, custodiada por personal de seguridad. Al ingresar se solicita una credencial oficial vigente y un registro con el nombre completo, área o persona a la que visita y hora de entrada. El personal de seguridad intercambia la credencial oficial del visitante por un pase de visitante, el cual está numerado por un identificador y un color del área que visita. La credencial oficial se queda con el personal de seguridad hasta que el visitante devuelve el pase de acceso y anote la hora de salida.

Alrededor de la coordinación se cuenta con cámaras de seguridad ubicadas estratégicamente que graban en tiempo real las 24 horas del día, la entrada principal, entrada al estacionamiento, entrada a las diferentes áreas, así como los principales pasillos.

#### **Seguridad perimetral interior**

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el director de la Dirección de Desarrollo de Sistemas para la Educación.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

Para la plataforma de LimeSurvey no se cuenta con actualización de datos que se obtienen de las encuestas realizadas.

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). El sistema operativo donde se hospedan las aplicaciones utiliza un sistema de cuentas de usuario local que cifra las contraseñas de los usuarios utilizando una función de Hash, la cual no es reversible. La plataforma LimeSurvey cifra las contraseñas de los usuarios utilizando MD5 y tiene un manejo estricto de los roles de usuario base con los cuales trabaja. La creación de nuevos perfiles de usuario es responsabilidad de los administradores de la plataforma y el Director de Desarrollo de Sistemas para la Educación autoriza la creación de estos. El departamento de Operaciones y Seguridad Informática lleva el control de los usuarios con permisos de administrador y la creación de nuevos perfiles dentro de la plataforma.

Los usuarios trabajan con el sistema mediante una vista web, por lo que no requieren de acceso al sistema operativo donde reside la aplicación. Las tareas de mantenimiento de la plataforma son realizadas mediante el acceso al servidor utilizando un mecanismo de llave pública/privada y solamente los administradores de la plataforma pueden realizar este proceso. La protección contra los accesos no autorizados se realiza mediante el filtrado de puertos y el sistema antes mencionado de llaves públicas y privadas, en donde el servidor no acepta accesos mediante contraseña.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

Las plataformas son respaldadas utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello por un promedio de treinta días tras lo cual, es almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas en condiciones óptimas para su funcionamiento. Su resguardo de estas cintas magnéticas es indefinido.



## IX. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de negocio el cual utiliza como fuente primordial los respaldos obtenidos de las plataformas en cintas magnéticas y en un servidor dedicado. En las pruebas de eficiencia que se realizan se ha garantizado la recuperación total de la plataforma en un periodo máximo de doce horas. Actualmente no se cuenta con un sitio redundante o alerno.

### 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

#### 7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-02	
Nombre del sistema)*	Encuestas CUAIEED - Limesurvey	
Recurso*	Descripción*	Control*
Gestor de usuarios del sistema	La plataforma Limesurvey cuenta con un gestor de usuarios que muestra la fecha en la que el usuario ingreso por primera y última vez	Solo los usuarios administradores tienen acceso para revisar y monitorear el estado de los usuarios
Nagios	Sistema de monitorización de redes, que vigila el estado y servicios dentro del servidor que hospeda la plataforma Limesurvey, alertando cuando se detectan intrusiones o procesos anormales.	Solo los administradores tienen acceso al sistema de monitoreo Nagios mediante acceso restringido.  Sistema de software abierto con Licencia GPLv2
Top	El comando top proporciona una vista dinámica en tiempo real de un sistema en ejecución y puede mostrar información de resumen del sistema, así como una lista de tareas que actualmente administra el kernel de Linux.	Este comando de monitoreo solo puede ser utilizado por los administradores del servidor donde está la plataforma Limesurvey con acceso restringido

#### 7.2. Procedimiento para la revisión de las medidas de seguridad

**Dirección de Desarrollo de Sistemas para la Educación**

<b>Identificador único*</b>	CUAIEED-DDSE-02	
<b>Nombre del sistema)*</b>	Encuestas CUAIEED - Limesurvey	
<b>Medida de seguridad*</b>	<b>Procedimiento*</b>	<b>Responsable*</b>
Revisión de permisos.	Revisiones de permisos dentro del servidor web y la aplicación.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de dos horas.
Script de respaldos de información.	Revisión aleatoria del contenido de los respaldos realizados.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización del sistema operativo.	Actualización a nuevas versiones de los paquetes del sistema operativo.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización de la aplicación.	Actualización de Plugins y componentes principales del núcleo de Limesurvey.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.

**7.3. Resultados de la evaluación y pruebas a las medidas de seguridad**

<b>Identificador único*</b>	CUAIEED-DDSE-02	
<b>Nombre del sistema)*</b>	Encuestas CUAIEED - Limesurvey	
<b>Medida de seguridad*</b>	<b>Resultado de evaluación*</b>	<b>Responsable*</b>
Revisión de permisos.	Se cuentan con los permisos adecuados.	Responsable: Departamento de Operaciones y Seguridad Informática.

Script de respaldos de información.	Los respaldos funcionan correctamente.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización del sistema operativo.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización de la aplicación.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.

#### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-02	
Nombre del sistema*	Encuestas CUAIEED - Limesurvey	
Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL.	Realizar la renovación anual del certificado SSL.	Responsable: Dirección de Sistemas para la Educación.
Actualización de la plataforma LimeSurvey.	Realizar el proceso de actualización periódica de la plataforma.	Responsable: Departamento de Operaciones y Seguridad Informática.

### 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

#### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

<b>Dirección de Desarrollo de Sistemas para la Educación</b>
--

<b>Identificador único*</b>	CUAIEED-DDSE-02		
<b>(Nombre del sistema) *</b>	Encuestas CUAIEED - Limesurvey		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Inicio: 19 de abril 2021 Término: 23 de mayo de 2021	Responsables de TI de las dependencias de la UNAM.

## 8.2. Programa de difusión de la protección a los datos personales

No se cuenta con un programa de difusión de la protección a los datos personales

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

Dirección de Desarrollo de Sistemas para la Educación			
<b>Identificador único*</b>	CUAIEED-DDSE-02		
<b>(Nombre del sistema) *</b>	Encuestas CUAIEED - Limesurvey		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
Actualización de la plataforma LimeSurvey a nuevas versiones.	Proceso de actualización hacia versiones superiores de la plataforma Limesurvey.	1 mes.	Total.

### 9.2. Actualización y mantenimiento de equipo de cómputo

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-02		
(Nombre del sistema) *	Encuestas CUAIEED - Limesurvey		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización del servidor físico.	<i>Cambio del servidor físico utilizado para crear máquinas virtuales donde se hospeda el sistema de Limesurvey</i>	3 meses.	Total.

### 9.3. Procesos para la conservación, preservación y respaldos de información

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-02	
(Nombre del sistema) *	Encuestas CUAIEED - Limesurvey	
Proceso*	Descripción*	Responsable*
Resguardo de cintas magnéticas.	<i>Las cintas magnéticas realizadas en la fase de respaldo automatizado son resguardadas de forma indefinida en un almacén.</i>	<i>Departamento de Operaciones y Seguridad Informática.</i>

### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección de Desarrollo de Sistemas para la Educación		
<b>Identificador único*</b>	CUAIEED-DDSE-02	
<b>(Nombre del sistema) *</b>	Encuestas CUAIEED - Limesurvey	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
Borrado seguro.	Se realiza un formato de bajo nivel al disco duro físico del hipervisor.	Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.

## Piensa Más Allá

### Introducción

Enseñar el pensamiento crítico ha representado un reto, al ser un proceso cognitivo complejo que involucra diversas habilidades y requiere de tiempo y práctica constante. Con la finalidad de incentivar este pensamiento en estudiantes del nivel medio superior y superior, la UNAM creó una aplicación móvil, sustentada en la estrategia “Crear y dudar” de Elbow (2009), que ha sido utilizada para el análisis de situaciones controversiales en diferentes contextos formativos.

La Web App “Piensa más allá” es una herramienta que almacena y gestiona escenarios diseñados por docentes de nivel medio superior y superior siguiendo los pasos de la metodología Creer y Dudar, con la intención de promover el pensamiento crítico de los estudiantes. En cada escenario se presenta un dilema ante el cual, el usuario debe adoptar una postura: a favor o en contra, mantener una postura empática para analizar la postura contraria a la elegida, reflexionar sobre algunos argumentos y evidencias e involucrarse en un proceso de autoevaluación de su propia manera de pensar.

### 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección de Desarrollo de Sistemas para la Educación	
<b>Identificador único*</b>	CUAIEED-DDSE-03
<b>(Nombre del sistema) *</b>	Piensa Más Allá
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre Apellidos Correo electrónico Fecha de nacimiento Genero País de residencia

	Nivel educativo Institución educativa Experiencia docente en años
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
<b>Nombre*:</b>	Mtro. Ricardo Arroyo Mendoza
<b>Cargo*:</b>	Director de la Dirección de Desarrollo de Sistemas para la Educación.
<b>Funciones*:</b>	Definir la arquitectura tecnológica necesaria para el funcionamiento y mantenimiento del sistema.
<b>Obligaciones*:</b>	Vigilar que el sistema cumpla con todas las medidas de seguridad técnica, físicas y administrativas.
	<b>Encargados<sup>2</sup>:</b>
<b>(Nombre del Encargado 1*)</b>	<b>Mtro. Eduardo López Molina</b>
<b>Cargo*:</b>	<b>Coordinador de Informática y Proyectos de Tecnologías de la Información</b>
<b>Funciones*:</b>	<ul style="list-style-type: none"> <li>• Desarrollador de sistemas para la educación.</li> <li>• Mejora continua, actualización, mantenimiento preventivo y correctivo de los sistemas de la Dirección de Desarrollo de Sistemas para la Educación.</li> </ul>
<b>Obligaciones*:</b>	Cumplir con la confidencialidad de los datos personales.
	<b>Usuarios:</b>
<b>(Nombre del Usuario 1*)</b>	Verónica Luna de la Luz
<b>Cargo*:</b>	Subdirectora de Innovación Educativa
<b>Funciones*:</b>	Capacitación a docentes y monitoreo del sistema Piensa Más Allá.
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos de Piensa Más Allá.

<sup>2</sup> Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único**	CUAIEED-DDSE-03
(Nombre del sistema *)	<b>Piensa Más Allá</b>
Tipo de soporte: *	Electrónico
Descripción: *	Base de datos
Características del lugar donde se resguardan los soportes: *	Alojamiento en el centro de datos de CUAIEED, dentro de diversas máquinas virtuales, el cual cuenta con temperatura controlada y acceso mediante un sistema biométrico

## 3. ANÁLISIS DE RIESGOS

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-03	
(Nombre del sistema) *	Piensa Más Allá	
Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor
Explotación de vulnerabilidades	Medio	Actualización de librerías y frameworks

## 4. ANÁLISIS DE BRECHA



(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-03	
Nombre del sistema) *	Piensa Más Allá	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Las contraseñas no tienen longitud mínima	Las contraseñas deben tener una longitud mínima de 8 caracteres	Se debe actualizar las contraseñas ya existentes y a su vez, agregar a los nuevos usuarios con contraseñas que cumplan el requisito mínimo de longitud
Contraseñas seguras de usuario	Las contraseñas de usuario deben ser únicas y rotadas constantemente para evitar el descubrimiento por medio de ataques de diccionario.	Cambio de contraseñas de usuario cada seis meses.
Cifrado de comunicaciones entre cliente y servidor	Uso de certificado de seguridad SSL/TLS en todas las comunicaciones realizadas por el desarrollo.	Uso en local de imágenes y scripts de javascript para la vista web.

### 5. PLAN DE TRABAJO

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-03

(Nombre del sistema) *	<i>Piensa Más Allá</i>		
Actividad*	Descripción*	Duración*	Cobertura*
<i>Mantenimiento preventivo</i>	<i>Revisión y actualización de código para nuevas versiones compatible con servidor y navegadores</i>	<i>20 horas</i> <i>Semestral</i>	<i>Los datos se encuentran con la seguridad adecuada para no ser consultados por un usuario no autenticado en el sistema</i>

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-03
(Nombre del sistema) *	<b>Piensa Más Allá</b>
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales mediante el traslado de redes electrónicas.

### I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No aplica, se tiene soporte electrónico en una base de datos.

## II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web, almacenando la fecha, hora, dirección IP, así como todas las acciones dentro del sistema. Los archivos de log que se encuentran dentro del sistema operativo y se rotan cada diez días, mientras que las bitácoras dentro de la base de datos se almacenan de forma indeterminada hasta el final de la vida útil del sistema. La integridad de las bitácoras se garantiza utilizando una suma de HASH. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática de la CUAIEED y las herramientas utilizadas para el análisis son AWK, SED y GREP.

## III. REGISTRO DE INCIDENTES

Los incidentes son reportados al Departamento de Operaciones y Seguridad Informática en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuentan con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

El tipo de soporte es electrónico por lo que la recuperación de la base de datos, la cual se encarga de almacenar los datos personales de los usuarios, es el proceso más importante; este consiste en recuperar el código del desarrollo junto con una copia de la base de datos obtenida en el proceso de respaldo programado.

Tras realizar la recuperación de los datos se realiza una comparación con un respaldo de la base de datos antes de ser comprometida para validar su estado y determinar la pertinencia de su uso. Si fue utilizado un respaldo para la recuperación se valida su integridad con una suma de HASH.

## V. ACCESO A LAS INSTALACIONES

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED en un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia y el área se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias. Las personas que acceden a laborar a las instalaciones son identificadas por una identificación oficial vigente.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación, este permite el acceso mediante el uso de biométricos (huella dactilar) para permitir el ingreso. El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el director de la Dirección de Sistemas para la Educación.

## VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El solicitante de una corrección de datos personales deberá de enviar un ticket a la mesa de ayuda correspondiente del sistema, tras identificarse como usuario, indicará el dato incorrecto seguido de los nuevos datos a actualizar. El cambio se realizará en un plazo no mayor a cuarenta y ocho horas tras ser recibida la solicitud.

## VII. PERFILES DE USUARIO Y CONTRASEÑAS

El modelo de control de acceso al sistema se encuentra basado en roles (perfiles). El sistema operativo donde se hospedan las aplicaciones utiliza un sistema de cuentas de usuario local que cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible. Los nuevos usuarios son creados a partir de un registro por parte del administrador del sistema. Los usuarios trabajan con el sistema mediante una vista web por lo que no requieren de acceso al sistema operativo donde vive la aplicación.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El sistema es respaldado utilizando un esquema de respaldo completo que incorpora el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 15 días). Los respaldos son almacenados de forma temporal en un servidor dedicado para ello por un promedio de treinta días, tras lo cual, es almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas en condiciones óptimas para su funcionamiento. El resguardo de las cintas magnéticas es indefinido.

## IX. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de la operación, el cual utiliza como fuente primordial los respaldos obtenidos del sistema en cintas magnéticas y en un servidor dedicado. En las pruebas de eficiencia que se realizan, se ha garantizado la recuperación total del sistema en un periodo máximo de doce horas. Actualmente, no se cuenta con un sitio redundante o alterno.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1. Herramientas y recursos para monitoreo de la protección de datos personales

*(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)*

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEFD-DDSE-03	
Nombre del sistema)*	Piensa Más Allá	
Recurso*	Descripción*	Control*
Bitácoras del sistema	Revisión aleatoria del contenido de los logs del sistema operativo y aplicación.	Se realiza una revisión no automatizada buscando patrones de ataque conocidos y secuencias de ataques conocidos como el descubrimiento de puertos y búsqueda de archivos de configuración conocidos.

*Responsables: Departamento de Operaciones y Seguridad Informática.*

### 7.2. Procedimiento para la revisión de las medidas de seguridad

*(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)*

<b>Dirección de Desarrollo de Sistemas para la Educación</b>		
<b>Identificador único*</b>	<i>CUAIEED-DDSE-03</i>	
<b>Nombre del sistema)*</b>	<i>Piensa Más Allá</i>	
<b>Medida de seguridad*</b>	<b>Procedimiento*</b>	<b>Responsable*</b>
<i>Revisión de permisos.</i>	<i>Revisiones de permisos dentro del servidor web y la aplicación.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de dos horas.</i>
<i>Scripts de respaldos de información.</i>	<i>Revisión aleatoria del contenido de los respaldos realizados.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.</i>
<i>Actualización del sistema operativo.</i>	<i>Actualización a nuevas versiones de los paquetes del sistema operativo.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.</i>
<i>Actualización de la aplicación.</i>	<i>Actualización de librerías y frameworks principales del sistema.</i>	<i>Responsable: Coordinador de Informática y Proyectos de Tecnologías de la Información.  Duración es de 20 horas.</i>

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-03	
Nombre del sistema) *	Piensa Más Allá	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Revisión de permisos.	Se cuentan con los permisos adecuados.	Responsable: Departamento de Operaciones y Seguridad Informática.
Scripts de respaldos de información.	Los respaldos funcionan correctamente.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización del sistema operativo.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización de la aplicación.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.

#### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-03
Nombre del sistema) *	Piensa Más Allá

Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL	Realizar la renovación anual del certificado SSL	Responsable: Dirección de Sistemas para la Educación

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

**8.1. Programa de capacitación a los responsables de seguridad de datos personales**  
(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-03		
(Nombre del sistema) *	Piensa Más Allá		
Actividad*	Descripción*	Duración*	Cobertura*
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Inicio: 19 de abril 2021 Término: 23 de mayo de 2021	Responsables de TI de las dependencias de la UNAM.

**8.2. Programa de difusión de la protección a los datos personales**  
(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

No existe un programa específico de difusión de la protección de datos personales

## 9. MEJORA CONTINUA

**9.1. Actualización y mantenimiento de sistemas de información**  
(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación			
<b>Identificador único*</b>	CUAIEED-DDSE-03		
<b>(Nombre del sistema) *</b>	Piensa Más Allá		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
<i>Creación de nuevos subsistemas/módulos</i>	<i>Desarrollo WEB para cumplir las nuevas necesidades del usuario, las cuales van surgiendo durante el uso de este.</i>	<i>50 horas cada 3 meses</i>	<i>Creación de reportes Automatización de procesos</i>

### 9.2. Actualización y mantenimiento de equipo de cómputo

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación			
<b>Identificador único*</b>	CUAIEED-DDSE-03		
<b>(Nombre del sistema) *</b>	Piensa Más Allá		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
<i>Actualización del servidor físico.</i>	<i>Cambio del servidor físico utilizado para crear máquinas virtuales donde vive el sistema alojado.</i>	<i>3 meses.</i>	<i>Total.</i>

### 9.3. Procesos para la conservación, preservación y respaldos de información

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)



Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-03	
(Nombre del sistema) *	Piensa Más Allá	
Proceso*	Descripción*	Responsable*
<i>Resguardo de cintas magnéticas.</i>	<i>Las cintas magnéticas realizadas en la fase de respaldo automatizado son resguardadas de forma indefinida en un almacén.</i>	<i>Departamento de Operaciones y Seguridad Informática.</i>

**9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos**  
*(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)*

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-03	
(Nombre del sistema) *	Piensa Más Allá	
Proceso*	Descripción*	Responsable*
<i>Borrado seguro.</i>	<i>Se realiza un formato de bajo nivel al disco duro físico del hipervisor.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.</i>

## **Argumente**

### **Introducción**

Es un sistema para fortalecer el ejercicio de la argumentación escrita, ya sea mediante grupos de estudio (incluyendo los escolares) o en comunidades de aprendizaje abiertas. Para ello se consideran dos espacios llamados Aula cerrada y aula abierta.

#### Aula cerrada

Genera la argumentación escrita e individual, a partir de las tesis, utilizando tarjetas de ideas.

Contempla 3 tipos de usuarios como es profesor, guía y alumno.

Permite crear, almacenar y organizar las tesis

Permite al profesor y al guía calificar y dar seguimiento individual y grupal a las argumentaciones

Permite a los alumnos compartir argumentos creados

Con el usuario profesor se pueden crear grupos de estudio para argumentar las tesis

#### Aulas abiertas

Permite la discusión argumentada de una tesis entre varias personas

Contempla dos tipos de usuarios como es observador y argumentador

Permite crear, almacenar y organizar las tesis

Como argumentados se pueden generar nuevas discusiones y participar en todas

Como observador se puede tener acceso a las tesis y a las discusiones argumentadas por otras personas

### 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único*</b>	CUAIEED-DDSE-04
<b>(Nombre del sistema) *</b>	<b>Argumete</b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre Apellido Paterno Apellido Materno Nivel académico Correo Código de Grupo (opcional)
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
<b>Nombre*:</b>	Mtro. Ricardo Arroyo
<b>Cargo*:</b>	Director de la Dirección de Desarrollo de Sistemas para la Educación.
<b>Funciones*:</b>	Definir la arquitectura tecnológica necesaria para el funcionamiento y mantenimiento del sistema.
<b>Obligaciones*:</b>	Vigilar que el sistema cumpla con todas las medidas de seguridad técnica, físicas y administrativas.
	<b>Encargados:</b>
<b>(Nombre del Encargado 1*)</b>	<b>Mtro. Eduardo López Molina</b>

<b>Cargo*:</b>	<b>Coordinador de Informática y Proyectos de Tecnologías de la Información</b>
<b>Funciones*:</b>	<ul style="list-style-type: none"> <li>• Desarrollador de sistemas para la educación.</li> <li>• Mejora continua, actualización, mantenimiento preventivo y correctivo de los sistemas de la Dirección de Desarrollo de Sistemas para la Educación.</li> </ul>
<b>Obligaciones*:</b>	Cumplir con la confidencialidad de los datos personales.
<b>(Nombre del Encargado 2*)</b>	Larisa Enríquez Vázquez
<b>Cargo*:</b>	Coordinadora de aprendizaje Autónomo y Adaptativo
<b>Funciones*:</b>	<ul style="list-style-type: none"> <li>• Decidir los usuarios con accesos administrativos al sistema.</li> <li>• Capacitar a docentes y monitorear el sistema Argumente.</li> </ul>
<b>Obligaciones*:</b>	Cumplir los reglamentos establecidos de Argumente.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

*(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)*

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único*</b>	<i>CUAIEED-DDSE-04</i>
<b>(Nombre del sistema *)</b>	<b>Argumente</b>
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos
<b>Características del lugar donde se resguardan los soportes: *</b>	Alojamiento en el centro de datos de CUAIEED dentro de diversas máquinas virtuales, el cual cuenta con temperatura controlada y acceso mediante un sistema biométrico en el centro de datos CUAIEED

## 3. ANÁLISIS DE RIESGOS

*(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)*

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-04	
Nombre del sistema) *	Argumente	
Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado.	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor.
Explotación de vulnerabilidades.	Medio	Actualización de librerías y frameworks

#### 4. ANÁLISIS DE BRECHA

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-04	
Nombre del sistema) *	Argumente	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Las contraseñas no tienen longitud mínima	Las contraseñas deben tener una longitud mínima de 8 caracteres	Se debe actualizar las contraseñas ya existentes y a su vez, agregar a los nuevos usuarios con contraseñas que cumplan el requisito mínimo de longitud

Contraseñas seguras de usuario	Las contraseñas de usuario deben ser únicas y rotadas constantemente para evitar el descubrimiento por medio de ataques de diccionario.	Cambio de contraseñas de usuario cada seis meses.
Cifrado de comunicaciones entre cliente y servidor	Uso de certificado de seguridad SSL/TLS en todas las comunicaciones realizadas por el desarrollo.	Uso en local de imágenes y scripts de javascript para la vista web.

## 5. PLAN DE TRABAJO

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-04		
(Nombre del sistema) *	Argumente		
Actividad*	Descripción*	Duración*	Cobertura*
Mantenimiento preventivo	Revisión y actualización de código para nuevas versiones compatible con servidor y navegadores	20 horas Semestral	Los datos se encuentran con la seguridad adecuada para no poder ser consultados por un usuario no autenticado en el sistema

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación

<b>Identificador único*</b>	CUAIEED-DDSE-04
<b>(Nombre del sistema) *</b>	<b>Argumente</b>
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
<b>Transferencias mediante el traslado de soportes físicos:</b>	No se realizan transferencias de datos personales mediante el traslado de soportes físicos
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No se realizan transferencias de datos personales mediante el traslado de redes electrónicas.

#### **I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

No aplica, se tiene soporte electrónico en una base de datos.

#### **II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web, almacenando la fecha, hora, dirección IP, así como todas las acciones dentro del sistema. Los archivos de log que se encuentran dentro del sistema operativo se rotan cada diez días mientras que las bitácoras dentro de la base de datos se almacenan de forma indeterminada hasta el final de la vida útil del sistema. La integridad de las bitácoras se garantiza utilizando una suma de HASH. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática, las herramientas utilizadas para el análisis son AWK, SED y GREP.

#### **III. REGISTRO DE INCIDENTES**

Los incidentes son reportados al Departamento de Operaciones y Seguridad Informática en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuentan con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

El tipo de soporte es electrónico por lo que la recuperación de la base de datos, la cual se encarga de almacenar los datos personales de los usuarios, es el proceso más importante. Este consiste en recuperar el código del desarrollo junto con una copia de la base de datos obtenida en el proceso de respaldo programado.

Tras realizar la recuperación de los datos se realiza una comparación con un respaldo de la base de datos antes de ser comprometida para validar su estado y determinar la pertinencia de su uso. Si fue utilizado un respaldo para la recuperación se valida su integridad con una suma de HASH.

#### **V. ACCESO A LAS INSTALACIONES**

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED otorgando una vigilancia en todas las instalaciones de veinticuatro horas al día. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, esta se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias. Las personas que acceden a laborar a las instalaciones son identificadas por una identificación oficial vigente.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación, este permite el acceso mediante el uso de biométricos (huella dactilar) para permitir el ingreso. El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el director de la Dirección de Sistemas para la Educación.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

El solicitante de una corrección de datos personales deberá de enviar un ticket a la mesa de ayuda correspondiente del sistema, tras identificarse como usuario, indicará el dato incorrecto seguido de los nuevos datos a actualizar. El cambio se realizará en un plazo no mayor a cuarenta y ocho horas tras ser recibida la solicitud.

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

El modelo de control de acceso al sistema se encuentra basado en roles (perfiles). El sistema operativo donde se hospedan las aplicaciones utiliza un sistema de cuentas de usuario local que cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible. Los nuevos usuarios son creados a partir de un registro por parte del administrador del sistema. Los usuarios trabajan con el sistema mediante una vista web por lo que no requieren de acceso al sistema operativo donde vive la aplicación.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

El sistema es respaldado utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello por un promedio de treinta días, tras lo cual, es almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas en condiciones óptimas para su funcionamiento. Su resguardo de estas cintas magnéticas es indefinido.

## **IX. PLAN DE CONTINGENCIA**

Se cuenta con un plan de contingencia que permite la continuidad de la operación, el cual utiliza como fuente primordial los respaldos obtenidos del sistema en cintas magnéticas y en un servidor dedicado. En las pruebas de eficiencia que se realizan, se ha garantizado la recuperación total del sistema en un periodo máximo de doce horas. Actualmente, no se cuenta con un sitio redundante o alterno.

## **7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD**

### **7.1. Herramientas y recursos para monitoreo de la protección de datos personales**

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-04	
Nombre del sistema) *	Argumente	
Recurso*	Descripción*	Control*
Bitácoras del sistema	Revisión aleatoria del contenido de los logs del sistema operativo y aplicación.	Se realiza una revisión no automatizada buscando patrones de ataque conocidos y secuencias de ataques conocidos como el descubrimiento de puertos y búsqueda de archivos de configuración conocidos.  Responsables: Departamento de Operaciones y Seguridad Informática.

## 7.2. Procedimiento para la revisión de las medidas de seguridad

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-04	
Nombre del sistema) *	Argumente	
Medida de seguridad*	Procedimiento*	Responsable*
Revisión de permisos.	Revisiones de permisos dentro del servidor web y la aplicación.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de dos horas.



Scripts de respaldos de información.	Revisión aleatoria del contenido de los respaldos realizados.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización del sistema operativo.	Actualización a nuevas versiones de los paquetes del sistema operativo.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización de la aplicación.	Actualización de librerías y frameworks principales del sistema.	Responsable: Coordinador de Informática y Proyectos de Tecnologías de la Información.  Duración es de 20 horas.

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-04	
Nombre del sistema) *	Argumente	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Revisión de permisos.	Se cuentan con los permisos adecuados.	Responsable: Departamento de Operaciones y Seguridad Informática.
Scripts de respaldos de información.	Los respaldos funcionan correctamente.	Responsable: Departamento de Operaciones y Seguridad Informática.

Actualización del sistema operativo.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización de la aplicación.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.

**7.4. Acciones para la corrección y actualización de las medidas de seguridad**  
(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-04	
Nombre del sistema) *	Argumente	
Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL.	Realizar la renovación anual del certificado SSL.	Responsable: Dirección de Sistemas para la Educación.

**8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN**

**8.1. Programa de capacitación a los responsables de seguridad de datos personales**  
(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-04		
(Nombre del sistema) *	Argumente		
Actividad*	Descripción*	Duración*	Cobertura*

Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Inicio: 19 de abril 2021 Término: 23 de mayo de 2021	Responsables de TI de las dependencias de la UNAM.
--	----------------	--	--

## 8.2. Programa de difusión de la protección a los datos personales

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

No existe un programa específico de difusión de la protección a los datos personales

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-04		
(Nombre del sistema) *	Argumente		
Actividad*	Descripción*	Duración*	Cobertura*
Creación de nuevos subsistemas/módulos	<i>Desarrollo WEB para cumplir las nuevas necesidades del usuario, las cuales van surgiendo durante el uso de este.</i>	<i>50 horas cada 3 meses</i>	<i>Creación de reportes Automatización de procesos</i>

### 9.2. Actualización y mantenimiento de equipo de cómputo

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

Dirección de Desarrollo de Sistemas para la Educación

<b>Identificador único*</b>	<i>CUAIEED-DDSE-04</i>		
<b>(Nombre del sistema) *</b>	<b>Argumente</b>		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
<i>Actualización del servidor físico.</i>	<i>Cambio del servidor físico utilizado para crear máquinas virtuales donde vive el sistema alojado.</i>	<i>3 años.</i>	<i>Total.</i>

### 9.3. Procesos para la conservación, preservación y respaldos de información

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

<b>Dirección de Desarrollo de Sistemas para la Educación</b>		
<b>Identificador único*</b>	<i>CUAIEED-DDSE-04</i>	
<b>(Nombre del sistema) *</b>	<b>Argumente</b>	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
<i>Resguardo de cintas magnéticas.</i>	<i>Las cintas magnéticas realizadas en la fase de respaldo automatizado son resguardadas de forma indefinida en un almacén.</i>	<i>Departamento de Operaciones y Seguridad Informática.</i>

### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

<b>Dirección de Desarrollo de Sistemas para la Educación</b>
--

<b>Identificador único*</b>	CUAIEED-DDSE-04	
<b>(Nombre del sistema) *</b>	Argumente	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
Borrado seguro.	Se realiza un formato de bajo nivel al disco duro físico del hipervisor.	Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.

### **Sistema de Información y Control Escolar (SIICOE)**

#### **Introducción**

SIICOE nace ante la necesidad de integrar los datos generales que se generan durante el proceso de inscripción y seguimiento del alumnado del bachillerato a distancia de la UNAM. A partir de esta situación, se comenzó a trabajar con el desarrollo de un sistema de información y control escolar con el objetivo de sistematizar y automatizar la información que se origina de las diferentes actividades académico-administrativas.

El sistema tiene la posibilidad de extenderse a las dependencias del SUAyED que no cuenten con un sistema de control escolar para las plataformas Moodle que usen.

#### **1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES**

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único*</b>	CUAIEED-DDSE-05
<b>(Nombre del sistema) *</b>	Sistema de Información y Control Escolar
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre, apellido paterno, apellido materno, correo electrónico, genero, estado civil, fecha de nacimiento, país, CURP, calle, no exterior, no interior, colonia, CP, país, entidad, teléfono, celular. Número de cuenta del alumno, RFC del docente, calificaciones.

<b>Responsable*:</b>	
<b>Nombre*:</b>	Mtro. Ricardo Arroyo Mendoza
<b>Cargo*:</b>	Dirección Desarrollo de Sistemas para la Educación
<b>Funciones*:</b>	Decidir el tratamiento de los datos personales, así como el contenido y uso del sistema.
<b>Obligaciones*:</b>	<ul style="list-style-type: none"> <li>- Decidir sobre la incorporación de nuevas funcionalidades en el sistema.</li> <li>- Asegurar que el sistema cumpla con las medidas de seguridad necesarias.</li> </ul>
	<b>Encargados:</b>
<b>(Nombre del Encargado 1*)</b>	Lic. José Ángel Linares Orrala
<b>Cargo*:</b>	Departamento de Desarrollo de Ecosistemas Educativos
<b>Funciones*:</b>	Realizar el proceso de software con la finalidad de atender las necesidades de la CUAIEED, dicha actividad abarca el desarrollo y mantenimiento del software implementado en la dependencia.
<b>Obligaciones*:</b>	Proporcionar la protección de los datos personales con mecanismos de seguridad en su desarrollo y mantenimiento.
	<b>Usuarios:</b>

<b>(Nombre del Usuario 1*)</b>	Lic. Dulce Yunue Sánchez Iniestra
<b>Cargo*:</b>	Coordinación de Extranjero, Cantera y Música (BUNAM)
<b>Funciones*:</b>	Registrar y dar seguimiento a la matriculación en las asignaturas a los alumnos del BUNAM.
<b>Obligaciones*:</b>	Cumplir con la obligación legal de resguardar los datos personales.
<b>(Nombre del Usuario 2*)</b>	Mtro. José Alberto Vargas Castillo
<b>Cargo*:</b>	Coordinación de Juntos en Línea (BUNAM)
<b>Funciones*:</b>	Registrar y dar seguimiento a la matriculación en las asignaturas a los alumnos del BUNAM.
<b>Obligaciones*:</b>	Cumplir con la obligación legal de resguardar los datos personales.
<b>(Nombre del Usuario 3*)</b>	Mtra. Lilia Donaji Naranjo Sánchez
<b>Cargo*:</b>	Departamento de Vinculación de Bachillerato a Distancia (BUNAM)
<b>Funciones*:</b>	Registrar y dar seguimiento a la matriculación en las asignaturas a los alumnos del BUNAM.
<b>Obligaciones*:</b>	Cumplir con la obligación legal de resguardar los datos personales.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-05
(Nombre del sistema *)	Sistema de Información y Control Escolar
Tipo de soporte: *	Electrónico
Descripción: *	Base de datos
Características del lugar donde se resguardan los soportes: *	Alojamiento en el centro de datos de CUAIEED dentro de diversas máquinas virtuales, el cual cuenta con acceso mediante un sistema biométrico, planta de energía eléctrica, sistema de respaldo de energía eléctrica ininterrumpida (UPS) y aire acondicionado seco.

### 3. ANÁLISIS DE RIESGOS

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-05	
(Nombre del sistema) *	Sistema de Información y Control Escolar	
Riesgo*	Impacto*	Mitigación*
Ataques de SQL-Injection	Alto	Actualización de la base de datos y verificación del código utilizado.
Robo de identidad	Medio	Documento de recomendaciones sobre el robo de identidad y cómo evitarlo. Asignar contraseñas complicadas. Implementar autenticación de dos pasos.
Vulnerabilidades propias del lenguaje/framework utilizado para el desarrollo de la aplicación	Medio	Actualización a versiones recientes/estables del lenguaje/framework. Mantenimiento continuo al código de la aplicación

### 4. ANÁLISIS DE BRECHA



Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-05	
(Nombre del sistema) *	Sistema de Información y Control Escolar	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Actualización de las librerías de seguridad del servidor.	Tras la liberación de algún parche, implementar los parches correspondientes inmediatamente tras una verificación de compatibilidad con la aplicación.	Reducir los tiempos para mantener la aplicación actualizada.
Mantener la base de datos de la aplicación actualizada.	Actualización periódica, cada 6 meses, de la base de datos.	Reducir los tiempos para mantener la aplicación actualizada.
Revisar accesos sobre los puertos del servidor.	Solo permitir la conexión a los puertos que se usan para la aplicación.	Actualizar la configuración de seguridad en los puertos del servidor.

## 5. PLAN DE TRABAJO

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-05		
(Nombre del sistema) *	Sistema de Información y Control Escolar		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización del lenguaje de programación o framework	Actualizar el lenguaje/framework de desarrollo de la aplicación y sus dependencias. Realizar exhaustivas pruebas de funcionalidad en busca de errores o problemas de compatibilidad de las dependencias. Verificar el correcto funcionamiento. Aplicar las actualizaciones en el servidor de producción.	6 meses	Total

**6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS**  
**I. TRANSFERENCIAS DE DATOS PERSONALES**

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-05
(Nombre del sistema) *	Sistema de Información y Control Escolar
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
Transferencias mediante el traslado de soportes físicos:	No aplica.
Transferencias mediante el traslado de soportes electrónicos:	No aplica.
Transferencias mediante el traslado sobre redes electrónicas:	No aplica.

**I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

SIICOE no realiza tratamiento de datos personales en soportes físicos, ya que se encuentra en medio electrónico por medio de una base de datos.

**II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Uso de los archivos log del servidor y la aplicación.

**III. REGISTRO DE INCIDENTES:**

Los incidentes son recabados por correo electrónico o chat de los usuarios que usan la aplicación.

1. Los usuarios dan aviso de un comportamiento inusual o error del sistema.
2. Se confirma el comportamiento inusual o error.
3. Se notifica al usuario del problema y por qué sucede.
4. Se le avisa de la fecha tentativa de corrección.

**V. ACCESO A LAS INSTALACIONES**

**1. Seguridad perimetral exterior (las instalaciones del área universitaria)**

El acceso a la coordinación es mediante un puesto de control en la entrada principal y única, custodiada por personal de seguridad, el cual, solicita una credencial oficial vigente y un registro con el nombre completo, área o persona a la que visita y la hora de entrada. El personal de seguridad intercambia la credencial oficial del visitante por un pase de visitante, el cual está numerado por un identificador y un color del área visitada. La credencial oficial se queda con el personal de seguridad hasta que el visitante devuelve el pase de acceso y anote la hora de salida.

Alrededor de la coordinación se cuenta con cámaras de seguridad ubicadas estratégicamente que graban en tiempo real las 24 horas del día, la entrada principal, entrada a las diferentes áreas, así como los pasillos más transitados.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos).

La aplicación SIICOE se encuentra dentro de un servidor que está alojado en el centro de datos de la coordinación. El centro de datos se encuentra en la planta baja, solo cuenta con una puerta de acceso que sirve de entrada y salida, el acceso está controlado y restringido por un sistema de ingreso con tres formas de acceso:

Un sistema biométrico: el uso de una huella dactilar (dedo índice).

Una clave: clave de 6 dígitos (una clave para cada usuario con acceso).

Una tarjeta de contacto: Tarjeta maestra que da acceso al contacto (Resguardada bajo llave en posesión de los administradores).

Al ingresar al centro de datos con alguna de las tres formas de acceso, el sistema toma una fotografía del usuario que ingresó y emite una alerta sobre el acceso, tanto si el ingreso fue válido o no. El sistema de ingreso guarda toda la información del acceso o intento de acceso en un sistema de bitácoras que indica: fecha, hora de ingreso, nombre del usuario, número de identificador único, tipo de acceso, si fue entrada o salida del centro de datos y si el acceso fue válido o no.

Así mismo existe una cámara de seguridad grabando las 24 horas y en tiempo real el centro de datos.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

Para la actualización de los datos en la aplicación SIICOE sólo se actualizan a petición de los usuarios que operan la aplicación y el encargado de realizar los cambios es el Departamento de Desarrollo de Ecosistemas Educativos.

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

El modelo de control de acceso a la aplicación se encuentra basado en roles (perfiles). El sistema operativo donde se hospeda la aplicación utiliza un sistema de cuentas de usuario local que cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible. La aplicación cifra las contraseñas de los usuarios creados.

Los nuevos usuarios son dados de alta por medio de una petición, realizada por los usuarios operativos y es enviada por correo electrónico o chat, el encargado de dar de alta y dar el visto bueno es el Departamento de Desarrollo de Ecosistemas Educativos.

Los usuarios trabajan con el sistema mediante una vista web por lo que no requieren de acceso al sistema operativo donde vive la aplicación. El mantenimiento se realiza mediante el acceso al servidor utilizando un mecanismo de llave pública/privada. La protección contra los accesos no autorizados se realiza mediante el filtrado de puertos y el sistema antes mencionado de llaves públicas y privadas en donde el servidor no acepta accesos mediante contraseña.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

La aplicación es respaldada utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello por un promedio de treinta días tras lo cual, es almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de

Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas en condiciones óptimas para su funcionamiento. Su resguardo de estas cintas magnéticas es indefinido.

## IX. PLAN DE CONTINGENCIA

Para asegurar la continuidad de la aplicación se utiliza como fuente de recuperación los respaldos obtenidos de la aplicación en cintas magnéticas y en un servidor dedicado. El funcionamiento total de la plataforma se garantiza en un tiempo máximo de 12 horas. No se cuenta con un sitio redundante o alternativo.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-05	
(Nombre del sistema) *	Sistema de Información y Control Escolar	
Recurso*	Descripción*	Control*
Bitácora del sistema	Revisión aleatoria	Revisar de manera aleatoria la bitácora con el fin de identificar algún comportamiento inusual en la aplicación

### 7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-05	
(Nombre del sistema) *	Sistema de Información y Control Escolar	
Medida de seguridad*	Procedimiento*	Responsable*
Respaldos de información	Revisión y validación del historial de respaldos de la aplicación	Departamento de Operaciones y Seguridad Informática
Aplicar actualizaciones de seguridad más recientes disponibles	Revisión y actualizaciones del sistema operativo	Departamento de Operaciones y Seguridad Informática

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-05	
(Nombre del sistema) *	Sistema de Información y Control Escolar	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Respaldos de información	Se cuenta con respaldos actualizados de la información de la aplicación.	Departamento de Operaciones y Seguridad Informática
Aplicar actualizaciones de seguridad más recientes disponibles.	El sistema operativo cuenta con las actualizaciones de seguridad más recientes.	Departamento de Operaciones y Seguridad Informática

#### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-05	
(Nombre del sistema) *	Sistema de Información y Control Escolar	
Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL	Renovación anual del certificado SSL para el subdominio donde se encuentra la aplicación	Departamento de Operaciones y Seguridad Informática
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la próxima versión estable	Departamento de Desarrollo de Ecosistemas Educativos

### 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

#### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-05

<b>(Nombre del sistema) *</b>		Sistema de Información y Control Escolar	
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Inicio: 19 de abril 2021 Término: 23 de mayo de 2021	Responsables de TI de las dependencias de la UNAM.

## 8.2. Programa de difusión de la protección a los datos personales

No se cuenta con un programa específico
---

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

Dirección de Desarrollo de Sistemas para la Educación			
<b>Identificador único*</b>		CUAIEED-DDSE-05	
<b>(Nombre del sistema) *</b>		Sistema de Información y Control Escolar	
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
Actualización de tecnologías de desarrollo	<p>Actualizar el framework de desarrollo de la aplicación y sus dependencias</p> <p>Realizar pruebas exhaustivas de funcionalidad en busca de errores o problemas de compatibilidad de las dependencias</p> <p>Verificar el correcto funcionamiento</p> <p>Aplicar las actualizaciones en el servidor de producción</p>	4 meses	Total

### 9.2. Actualización y mantenimiento de equipo de cómputo

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-05		
(Nombre del sistema) *	Sistema de Información y Control Escolar		
Actividad*	Descripción*	Duración*	Cobertura*
Adquisición de equipo de cómputo para desarrollo de software	Solicitud de compra de nuevo equipo de cómputo para desarrollo de software	5 años	Total

### 9.3. Procesos para la conservación, preservación y respaldos de información

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-05	
(Nombre del sistema) *	Sistema de Información y Control Escolar	
Proceso*	Descripción*	Responsable*
Ejecución del script en el servidor de respaldos	El script se conecta al servidor de producción donde está hospedada la aplicación Se realiza la sincronización sobre la carpeta donde se encuentra el código Se realiza una copia de la base de datos Se guardan los datos en el servidor de respaldos	Departamento de Operaciones y Seguridad Informática.  Tiempo: 1 día

### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-05
(Nombre del sistema) *	Sistema de Información y Control Escolar

Proceso*	Descripción*	Responsable*
Borrado seguro.	Se realiza un formato de bajo nivel al disco duro físico del hipervisor.	Departamento de Operaciones y Seguridad Informática.  Tiempo máximo de 24 horas.

## **Sistema de Administración y Seguimiento de Proyectos (SASP)**

### **Introducción**

SASP atiende la solicitud de tener un sistema donde se recopile información sobre los proyectos de la CUAIEED y las colaboraciones que se generen con la misma.

El sistema permite un seguimiento en las siguientes etapas a considerar:

1. Inicial. Revisión y aprobación de proyectos.
2. Desarrollo. Alta de servicios profesionales y recursos materiales,
3. Cierre. Generación de reportes estadísticos y financieros.

### **1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES**

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único*</b>	CUAIEED-DDSE-06
<b>(Nombre del sistema) *</b>	Sistema de Administración y Seguimiento de Proyectos
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre, apellidos, correo electrónico, RFC. Documentos: INE, CURP, constancia fiscal, comprobante de domicilio, bancario, estudios y CV.
<b>Responsable*:</b>	
<b>Nombre*:</b>	Mtro. Ricardo Arroyo Mendoza
<b>Cargo*:</b>	Dirección Desarrollo de Sistemas para la Educación
<b>Funciones*:</b>	Decidir el tratamiento de los datos personales, así como el contenido y uso del sistema.



<b>Obligaciones*:</b>	<ul style="list-style-type: none"> <li>- Decidir sobre la incorporación de nuevas funcionalidades en el sistema.</li> <li>- Asegurar que el sistema cumpla con las medidas de seguridad necesarias.</li> </ul>
	<b>Encargados:</b>
<b>(Nombre del Encargado 1*)</b>	Lic. José Ángel Linares Orrala
<b>Cargo*:</b>	Departamento de Desarrollo de Ecosistemas Educativos
<b>Funciones*:</b>	Realizar el proceso de software con la finalidad de atender las necesidades de la CUAIEED, dicha actividad abarca el desarrollo y mantenimiento del software implementado en la dependencia.
<b>Obligaciones*:</b>	Proporcionar la protección de los datos personales con mecanismos de seguridad en su desarrollo y mantenimiento.
	<b>Usuarios:</b>
<b>(Nombre del Usuario 1*)</b>	Lic. Lilia Paola Arredondo González
<b>Cargo*:</b>	Área de Contratación de Servicios Profesionales (CUAIEED)
<b>Funciones*:</b>	<p>Definir los perfiles de usuario con los diferentes roles de acceso.</p> <p>Operar el sistema en conjunto con los enlaces de las direcciones y áreas de la CUAIEED.</p> <p>Definir la funcionalidad y la información personal que se requiere manejar en el sistema</p>
<b>Obligaciones*:</b>	Cumplir con la obligación legal de resguardar los datos personales.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección de Desarrollo de Sistemas para la Educación

<b>Identificador único*</b>	CUAIEED-DDSE-06
<b>(Nombre del sistema *)</b>	Sistema de Administración y Seguimiento de Proyectos
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos
<b>Características del lugar donde se resguardan los soportes: *</b>	Alojamiento en el centro de datos de CUAIEED dentro de diversas máquinas virtuales, el cual cuenta con acceso mediante un sistema biométrico, planta de energía eléctrica, sistema de respaldo de energía eléctrica ininterrumpida (UPS) y aire acondicionado seco.

### 3. ANÁLISIS DE RIESGOS

Dirección de Desarrollo de Sistemas para la Educación		
<b>Identificador único*</b>	CUAIEED-DDSE-06	
<b>(Nombre del sistema) *</b>	Sistema de Administración y Seguimiento de Proyectos	
<b>Riesgo*</b>	<b>Impacto*</b>	<b>Mitigación*</b>
Ataques de <i>SQL-Injection</i>	Alto	Actualización de la base de datos y verificación del código utilizado.
Robo de identidad	Medio	Documento de recomendaciones sobre el robo de identidad y cómo evitarlo.  Asignar contraseñas complicadas.  Implementar autenticación de dos pasos.

Vulnerabilidades propias del lenguaje/framework utilizado para el desarrollo de la aplicación	Medio	Actualización a versiones recientes/estables del lenguaje/framework  Mantenimiento continuo al código de la aplicación
---	-------	--

#### 4. ANÁLISIS DE BRECHA

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-06	
(Nombre del sistema) *	Sistema de Administración y Seguimiento de Proyectos	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Actualización de las librerías de seguridad del servidor.	Tras la liberación de algún parche, implementar los parches correspondientes inmediatamente tras una verificación de compatibilidad con la aplicación	Reducir los tiempos para mantener la aplicación actualizada.
Mantener la base de datos de la aplicación actualizada.	Actualización periódica, cada 6 meses, de la base de datos.	Reducir los tiempos para mantener la aplicación actualizada.
Revisar accesos sobre los puertos del servidor	Solo permitir la conexión a los puertos que se usan para la aplicación	Actualizar la configuración de seguridad en los puertos del servidor.

#### 5. PLAN DE TRABAJO

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-06		
(Nombre del sistema) *	Sistema de Administración y Seguimiento de Proyectos		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización del lenguaje de programación o framework	<p>Actualizar el lenguaje/framework de desarrollo de la aplicación y sus dependencias</p> <p>Realizar exhaustivas pruebas de funcionalidad en busca de errores o problemas de compatibilidad de las dependencias</p> <p>Verificar el correcto funcionamiento</p> <p>Aplicar las actualizaciones en el servidor de producción</p>	6 meses	Total

**6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS**  
**I. TRANSFERENCIAS DE DATOS PERSONALES**

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-06
(Nombre del sistema) *	Sistema de Administración y Seguimiento de Proyectos
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	

<b>Transferencias mediante el traslado de soportes físicos:</b>	No aplica.
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No aplica.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No aplica.

## **I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

SASP no realiza tratamiento de datos personas es soportes físicos, ya que se encuentra en medio electrónico por medio de una base de datos.

## **II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Uso de los archivos log del servidor y la aplicación.

## **III. REGISTRO DE INCIDENTES:**

Los incidentes son recabados por correo electrónico o chat de los usuarios que usan la aplicación.

1. Los usuarios dan aviso de un comportamiento inusual o error del sistema.
2. Se confirma el comportamiento inusual o error.
3. Se notifica al usuario del problema y por qué sucede.
4. Se le avisa de la fecha tentativa de corrección.

## **V. ACCESO A LAS INSTALACIONES**

<p>1. Seguridad perimetral exterior (las instalaciones del área universitaria):</p> <p>El acceso a la coordinación es mediante un puesto de control en la entrada principal y única, custodiada por personal de seguridad, el cual, solicita una credencial oficial vigente y un registro con el nombre completo, área o persona a la que visita, hora de entrada. El personal de seguridad intercambia la credencial oficial del visitante por un pase de visitante, la cual está numerada por un identificador y un color del área el cual visita. La credencial oficial se queda con el personal de seguridad hasta que el visitante devuelve el pase de acceso y anoté la hora de salida.</p> <p>Alrededor de la coordinación se cuenta con cámaras de seguridad ubicadas estratégicamente que graban en tiempo real las 24 horas del día, la entrada principal, entrada a las diferentes áreas, así como los pasillos más transitados.</p>
<p>2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):</p> <p>La aplicación SASP se encuentra dentro de un servidor que está dentro del centro de datos de la coordinación. El centro de datos se encuentra la planta baja, solo cuenta con una puerta de acceso que sirve de entrada y salida, el acceso está controlado y restringido por un sistema de ingreso con tres formas de acceso:</p> <p>Un sistema biométrico: el uso de una huella dactilar (dedo índice)</p> <p>Una clave: clave de 6 dígitos (una clave para cada usuario con acceso)</p> <p>Una tarjeta de contacto: Tarjeta maestra que da acceso al contacto (Resguardada bajo llave en posesión de los administradores)</p>

Al ingresar al centro de datos con alguna de las tres formas de acceso, el sistema toma una fotografía del usuario que ingresó y emite una alerta sobre el acceso, tanto si el ingreso fue válido o no. El sistema de ingreso guarda toda la información del acceso o intento de acceso en un sistema de bitácoras que indica: fecha, hora de ingreso, nombre del usuario, número de identificador único, tipo de acceso, si fue entrada o salida del centro de datos y si el acceso fue válido o no. Así mismo existe una cámara de seguridad grabando las 24 horas y en tiempo real el centro de datos.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

Para la actualización de los datos en la aplicación SASP solo se actualizan a petición de los usuarios que utilizan la aplicación y el encargado de realizar los cambios es el Departamento de Desarrollo de Ecosistemas Educativos. Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

El modelo de control de acceso a la aplicación se encuentra basado en roles (perfiles). El sistema operativo donde se hospeda la aplicación utiliza un sistema de cuentas de usuario local que cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible. La aplicación cifra las contraseñas de los usuarios creados.

Los nuevos usuarios son dados de alta por medio de una petición, realizada por los usuarios operativos y es enviada por correo electrónico o chat, el encargado de dar de alta y dar el visto bueno es el Departamento de Desarrollo de Ecosistemas Educativos.

Los usuarios trabajan con el sistema mediante una vista web por lo que no requieren de acceso al sistema operativo donde vive la aplicación. El mantenimiento se realiza mediante el acceso al servidor utilizando un mecanismo de llave pública/privada. La protección contra los accesos no autorizados se realiza mediante el filtrado de puertos y el sistema antes mencionado de llaves públicas y privadas en donde el servidor no acepta accesos mediante contraseña.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

La aplicación es respaldada utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello por un promedio de treinta días tras lo cual, es almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello, que mantiene las cintas en condiciones óptimas para su funcionamiento. El resguardo de estas cintas magnéticas es indefinido.

## **IX. PLAN DE CONTINGENCIA**

Para asegurar la continuidad de la aplicación se utiliza como fuente de recuperación los respaldos obtenidos de la aplicación en cintas magnéticas y en un servidor dedicado. El funcionamiento total de la plataforma se garantiza en un tiempo máximo de 12 horas. No se cuenta con un sitio redundante o alterno.

## **7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD**

### **7.1. Herramientas y recursos para monitoreo de la protección de datos personales**

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-06	
(Nombre del sistema) *	Sistema de Administración y Seguimiento de Proyectos	
Recurso*	Descripción*	Control*
Bitácora del sistema	Revisión aleatoria	Revisar de manera aleatoria la bitácora con el fin de identificar algún comportamiento inusual en la aplicación

## 7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-06	
(Nombre del sistema) *	Sistema de Administración y Seguimiento de Proyectos	
Medida de seguridad*	Procedimiento*	Responsable*
Respaldos de información	Revisión y validación del historial de respaldos de la aplicación	Departamento de Operaciones y Seguridad Informática
Aplicar actualizaciones de seguridad más recientes disponibles	Revisión y actualizaciones del sistema operativo	Departamento de Operaciones y Seguridad Informática

## 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-06	
(Nombre del sistema) *	Sistema de Administración y Seguimiento de Proyectos	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Respaldos de información	Se cuenta con respaldos actualizados de la información de la aplicación.	Departamento de Operaciones y Seguridad Informática
Aplicar actualizaciones de seguridad más recientes disponibles	El sistema operativo cuenta con las actualizaciones de seguridad más recientes	Departamento de Operaciones y Seguridad Informática

#### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-06	
(Nombre del sistema) *	Sistema de Administración y Seguimiento de Proyectos	
Medida de seguridad*	Acciones*	Responsable*



Uso de certificados SSL	Renovación anual del certificado SSL para el subdominio donde se encuentra la aplicación	Departamento de Operaciones y Seguridad Informática
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la próxima versión estable	Departamento de Desarrollo de Ecosistemas Educativos

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-06		
(Nombre del sistema) *	Sistema de Administración y Seguimiento de Proyectos		
Actividad*	Descripción*	Duración*	Cobertura*
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Inicio: 19 de abril 2021 Término: 23 de mayo de 2021	Responsables de TI de las dependencias de la UNAM.

### 8.2. Programa de difusión de la protección a los datos personales

No se cuenta con un programa específico de difusión.
--

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

<b>Dirección de Desarrollo de Sistemas para la Educación</b>			
<b>Identificador único*</b>	CUAIEED-DDSE-06		
<b>(Nombre del sistema) *</b>	Sistema de Administración y Seguimiento de Proyectos		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
Actualización de tecnologías de desarrollo	<p>Actualizar el framework de desarrollo de la aplicación y sus dependencias</p> <p>Realizar exhaustivas pruebas de funcionalidad en busca de errores o problemas de compatibilidad de las dependencias</p> <p>Verificar el correcto funcionamiento</p> <p>Aplicar las actualizaciones en el servidor de producción</p>	1 mes	Total

## 9.2. Actualización y mantenimiento de equipo de cómputo

<b>Dirección de Desarrollo de Sistemas para la Educación</b>			
<b>Identificador único*</b>	CUAIEED-DDSE-06		
<b>(Nombre del sistema) *</b>	Sistema de Administración y Seguimiento de Proyectos		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>

Adquisición de equipo de cómputo para desarrollo de software	Solicitud de compra de nuevo equipo de cómputo para desarrollo de software	5 años	Total
--	--	--------	-------

### 9.3. Procesos para la conservación, preservación y respaldos de información

Dirección de Desarrollo de Sistemas para la Educación		
<b>Identificador único*</b>	CUAIEED-DDSE-06	
<b>(Nombre del sistema) *</b>	Sistema de Administración y Seguimiento de Proyectos	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
Ejecución del script en el servidor de respaldos	El script se conecta al servidor de producción donde está hospedada la aplicación Se realiza la sincronización sobre la carpeta donde se encuentra el código Se realiza una copia de la base de datos Se guardan los datos en el servidor de respaldos	Departamento de Operaciones y Seguridad Informática.  Tiempo: 1 día

### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección de Desarrollo de Sistemas para la Educación	
<b>Identificador único*</b>	CUAIEED-DDSE-06

<b>(Nombre del sistema) *</b>	Sistema de Administración y Seguimiento de Proyectos	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
Borrado seguro.	Se realiza un formato de bajo nivel al disco duro físico del hipervisor.	Departamento de Operaciones y Seguridad Informática.  Tiempo máximo de 24 horas.

## **Aulas Virtuales**

### **Introducción**

Aulas Virtuales es un servicio para que los docentes de la UNAM soliciten una licencia de las herramientas tecnológicas ofrecidas: Moodle o Zoom; con el fin de que sean usadas en la impartición de clases, seminarios, eventos y otras actividades académicas.

Durante la contingencia sanitaria, la planta docente de las distintas dependencias de la UNAM encontró en Aulas Virtuales una solución expedita para la impartición de clases remotas de emergencia.

### **1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES**

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único*</b>	CUAIEED-DDSE-07
<b>(Nombre del sistema) *</b>	Aulas Virtuales
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre, apellido paterno, apellido materno, correo electrónico, RFC, número de trabajador (UNAM), dependencia de adscripción.
<b>Responsable*:</b>	
<b>Nombre*:</b>	Mtro. Ricardo Arroyo Mendoza
<b>Cargo*:</b>	Dirección Desarrollo de Sistemas para la Educación

<b>Funciones*:</b>	Decidir el tratamiento de los datos personales, así como el contenido y uso del sistema.
<b>Obligaciones*:</b>	- Decidir sobre la incorporación de nuevas funcionalidades en el sistema.  - Asegurar que el sistema cumpla con las medidas de seguridad necesarias.
	Encargados:
<b>(Nombre del Encargado 1*)</b>	Lic. José Ángel Linares Orrala
<b>Cargo*:</b>	Departamento de Desarrollo de Ecosistemas Educativos
<b>Funciones*:</b>	Realizar el proceso de software con la finalidad de atender las necesidades de la CUAIEED, dicha actividad abarca el desarrollo y mantenimiento del software implementado en la dependencia.
<b>Obligaciones*:</b>	Proporcionar la protección de los datos personales con mecanismos de seguridad en su desarrollo y mantenimiento.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único*</b>	CUAIEED-DDSE-07
<b>(Nombre del sistema *)</b>	Aulas Virtuales
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos
<b>Características del lugar donde se resguardan los soportes: *</b>	Alojamiento en el centro de datos de CUAIEED dentro de diversas máquinas virtuales, el cual cuenta con acceso mediante un sistema biométrico, planta de energía eléctrica, sistema de respaldo de energía eléctrica ininterrumpida (UPS) y aire acondicionado seco.

### 3. ANÁLISIS DE RIESGOS

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-07	
(Nombre del sistema) *	Aulas Virtuales	
Riesgo*	Impacto*	Mitigación*
Robo de identidad	Medio	<p>Documento de recomendaciones sobre el robo de identidad y cómo evitarlo.</p> <p>Implementar la validación de usuario de dos pasos.</p>
Vulnerabilidades propias del lenguaje/framework utilizado para el desarrollo de la aplicación	Medio	<p>Actualización a versiones recientes/estables del lenguaje/framework</p> <p>Mantenimiento continuo al código de la aplicación</p>

### 4. ANÁLISIS DE BRECHA

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-07	
(Nombre del sistema) *	Aulas Virtuales	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*

Actualizar de las librerías de seguridad del servidor.	Tras la liberación de algún parche, implementar los parches correspondientes inmediatamente tras una verificación de compatibilidad con la aplicación	Reducir los tiempos para mantener la aplicación actualizada.
Mantener la base de datos de la aplicación actualizada.	Actualización periódica, cada 6 meses, de la base de datos.	Reducir los tiempos para mantener la aplicación actualizada.
Revisar accesos sobre los puertos del servidor	Solo permitir la conexión a los puertos que se usan para la aplicación	Actualizar la configuración de seguridad en los puertos del servidor.

## 5. PLAN DE TRABAJO

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-07		
(Nombre del sistema) *	Aulas Virtuales		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización del lenguaje de programación o framework	<p>Actualizar el lenguaje/framework de desarrollo de la aplicación y sus dependencias</p> <p>Realizar exhaustivas pruebas de funcionalidad en busca de errores o problemas de compatibilidad de las dependencias</p> <p>Verificar el correcto</p>	6 meses	Total

	funcionamiento		
	Aplicar las actualizaciones en el servidor de producción		

**6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS**  
**I. TRANSFERENCIAS DE DATOS PERSONALES**

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único*</b>	<b>CUAIEED-DDSE-07</b>
<b>(Nombre del sistema) *</b>	<b>Aulas Virtuales</b>
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
<b>Transferencias mediante el traslado de soportes físicos:</b>	No aplica.
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No aplica.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No aplica.

**I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

Aulas Virtuales no realiza tratamiento de datos personas es soportes físicos, ya que se encuentra en medio electrónico por medio de una base de datos.

**II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Uso de los archivos log del servidor y la aplicación.

**III. REGISTRO DE INCIDENTES:**

Los incidentes son atendidos por un sistema de tickets.

Los usuarios dan aviso de un comportamiento inusual o error del sistema.

1. Se confirma el comportamiento inusual o error.
2. Se notifica al usuario del problema y por qué sucede.
3. Se le avisa de la fecha tentativa de corrección.

**V. ACCESO A LAS INSTALACIONES**



#### 1. Seguridad perimetral exterior (las instalaciones del área universitaria):

El acceso a la coordinación es mediante un puesto de control en la entrada principal y única, custodiada por personal de seguridad, el cual, solicita una credencial oficial vigente y un registro con el nombre completo, área o persona a la que visita, hora de entrada. El personal de seguridad intercambia la credencial oficial del visitante por un pase de visitante, la cual está numerada por un identificador y un color del área el cual visita. La credencial oficial se queda con el personal de seguridad hasta que el visitante devuelve el pase de acceso y anota la hora de salida.

Alrededor de la coordinación se cuenta con cámaras de seguridad ubicadas estratégicamente que graban en tiempo real las 24 horas del día, la entrada principal, entrada a las diferentes áreas, así como los pasillos más transitados.

#### 2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

La aplicación Aulas Virtuales se encuentra dentro de un servidor que está dentro del centro de datos de la coordinación. El centro de datos se encuentra la planta baja, solo cuenta con una puerta de acceso que sirve de entrada y salida, el acceso está controlado y restringido por un sistema de ingreso con tres formas de acceso:

Un sistema biométrico: el uso de una huella dactilar (dedo índice)

Una clave: clave de 6 dígitos (una clave para cada usuario con acceso)

Una tarjeta de contacto: Tarjeta maestra que da acceso al contacto (Resguardada bajo llave en posesión de los administradores)

Al ingresar al centro de datos con alguna de las tres formas de acceso, el sistema toma una fotografía del usuario que ingresó y emite una alerta sobre el acceso, tanto si el ingreso fue válido o no.

El sistema de ingreso guarda toda la información del acceso o intento de acceso en un sistema de bitácoras que indica: fecha, hora de ingreso, nombre del usuario, número de identificador único, tipo de acceso, si fue entrada o salida del centro de datos y si el acceso fue válido o no.

Así mismo existe una cámara de seguridad grabando las 24 horas y en tiempo real el centro de datos.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

Para la actualización de los datos en la aplicación de Aulas Virtuales solo se actualizan a petición de los usuarios que utilizan la aplicación y el encargado de realizar los cambios es el Departamento de Desarrollo de Ecosistemas Educativos.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

El modelo de control de acceso a la aplicación se encuentra basado en reglas definidas desde el inicio del desarrollo. El sistema operativo donde vive la aplicación utiliza un sistema de cuentas de usuario local que cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible. Los nuevos usuarios se auto registran desde la aplicación y son ellos mismos en definir su contraseña. Los usuarios trabajan con el sistema mediante una vista web por lo que no requieren de acceso al sistema operativo donde vive la aplicación. El mantenimiento se realiza mediante el acceso al servidor utilizando un mecanismo de llave pública/privada. La protección contra los accesos no autorizados se realiza mediante el filtrado de puertos y el sistema antes mencionado de llaves públicas y privadas en donde el servidor no acepta accesos mediante contraseña.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

La aplicación es respaldada utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello por un promedio de treinta días tras lo cual, es almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas en condiciones óptimas para su funcionamiento. Su resguardo de estas cintas magnéticas es indefinido.

## IX. PLAN DE CONTINGENCIA

Para asegurar la continuidad de la aplicación se utiliza como fuente de recuperación los respaldos obtenidos de la aplicación en cintas magnéticas y en un servidor dedicado. El funcionamiento total de la plataforma se garantiza en un tiempo máximo de 12 horas. No se cuenta con un sitio redundante o alternativo.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEDD-DDSE-07	
(Nombre del sistema) *	Aulas Virtuales	
Recurso*	Descripción*	Control*
Bitácora del sistema	Revisión aleatoria	Revisar de manera aleatoria la bitácora con el fin de identificar algún comportamiento inusual en la aplicación

### 7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección de Desarrollo de Sistemas para la Educación		
---	--	--

<b>Identificador único*</b>	<b>CUAIEED-DDSE-07</b>	
<b>(Nombre del sistema) *</b>	<b>Aulas Virtuales</b>	
<b>Medida de seguridad*</b>	<b>Procedimiento*</b>	<b>Responsable*</b>
Respaldos de información	Revisión y validación del historial de respaldos de la aplicación	Departamento de Operaciones y Seguridad Informática
Aplicar actualizaciones de seguridad más recientes disponibles	Revisión y actualizaciones del sistema operativo	Departamento de Operaciones y Seguridad Informática

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

<b>Dirección de Desarrollo de Sistemas para la Educación</b>		
<b>Identificador único*</b>	<b>CUAIEED-DDSE-07</b>	
<b>(Nombre del sistema) *</b>	<b>Aulas Virtuales</b>	
<b>Medida de seguridad*</b>	<b>Resultado de evaluación*</b>	<b>Responsable*</b>
Respaldos de información	Se cuenta con respaldos actualizados de la información de la aplicación.	Departamento de Operaciones y Seguridad Informática
Aplicar actualizaciones de seguridad más recientes	El sistema operativo cuenta con las actualizaciones de	Departamento de Operaciones y Seguridad Informática

disponibles	seguridad más recientes
-------------	-------------------------

#### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-07	
(Nombre del sistema) *	Aulas Virtuales	
Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL	Renovación anual del certificado SSL para el subdominio donde se encuentra la aplicación	Departamento de Operaciones y Seguridad Informática
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la próxima versión estable	Departamento de Desarrollo de Ecosistemas Educativos

### 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

#### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-07
(Nombre del sistema) *	Aulas Virtuales

Actividad*	Descripción*	Duración*	Cobertura*
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Inicio: 19 de abril 2021 Término: 23 de mayo de 2021	Responsables de TI de las dependencias de la UNAM.

## 8.2. Programa de difusión de la protección a los datos personales

No se cuenta con un programa de difusión.

No se cuenta con un programa específico de difusión de la protección de datos personales

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-07		
(Nombre del sistema) *	Aulas Virtuales		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización de tecnologías de desarrollo	<p>Actualizar el framework de desarrollo de la aplicación y sus dependencias</p> <p>Realizar exhaustivas pruebas de funcionalidad en busca de errores o problemas de compatibilidad de las dependencias</p> <p>Verificar el correcto</p>	2 meses	Total

	funcionamiento  Aplicar las actualizaciones en el servidor de producción		
--	--	--	--

### 9.2. Actualización y mantenimiento de equipo de cómputo

<b>Dirección de Desarrollo de Sistemas para la Educación</b>			
<b>Identificador único*</b>	<b>CUAIEED-DDSE-07</b>		
<b>(Nombre del sistema) *</b>	<b>Aulas Virtuales</b>		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
Adquisición de equipo de cómputo para desarrollo de software	Solicitud de compra de nuevo equipo de cómputo para desarrollo de software	5 años	Total

### 9.3. Procesos para la conservación, preservación y respaldos de información

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único*</b>	<b>CUAIEED-DDSE-07</b>
<b>(Nombre del sistema) *</b>	<b>Aulas Virtuales</b>

Proceso*	Descripción*	Responsable*
Ejecución del script en el servidor de respaldos	El script se conecta al servidor de producción donde está hospedada la aplicación Se realiza la sincronización sobre la carpeta donde se encuentra el código Se realiza una copia de la base de datos Se guardan los datos en el servidor de respaldos	Departamento de Operaciones y Seguridad Informática.  Tiempo: 1 día

#### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-07	
(Nombre del sistema) *	Aulas Virtuales	
Proceso*	Descripción*	Responsable*
Borrado seguro.	Se realiza un formato de bajo nivel al disco duro físico del hipervisor.	Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.

### DespegApp

#### Introducción

DespegApp es un sistema que fue desarrollado para que los expertos de las universidades que están dentro de la Red de Innovación Educativa RIE360, implementen recursos educativos y creen contenidos con la finalidad de que los alumnos de formación universitaria les ayuden a desarrollar habilidades de aprendizaje.

#### 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único*</b>	<b>CUAIEED-DDSE-08</b>
<b>(Nombre del sistema A1) *</b>	<b>DespegApp</b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre, apellido, correo electrónico, pronombre, campus (dependencia universitaria).
<b>Responsable*:</b>	
<b>Nombre*:</b>	Mtro. Ricardo Arroyo Mendoza
<b>Cargo*:</b>	Dirección Desarrollo de Sistemas para la Educación
<b>Funciones*:</b>	Decidir el tratamiento de los datos personales, así como el contenido y uso del sistema.
<b>Obligaciones*:</b>	<ul style="list-style-type: none"> <li>- Decidir sobre la incorporación de nuevas funcionalidades en el sistema.</li> <li>- Asegurar que el sistema cumpla con las medidas de seguridad necesarias.</li> </ul>
	Encargados:
<b>(Nombre del Encargado 1*)</b>	Lic. José Ángel Linares Orrala
<b>Cargo*:</b>	Departamento de Desarrollo de Ecosistemas Educativos
<b>Funciones*:</b>	Realizar el proceso de software con la finalidad de atender las necesidades de la CUAIEED, dicha actividad abarca el desarrollo y mantenimiento del software implementado en la dependencia.
<b>Obligaciones*:</b>	Proporcionar la protección de los datos personales con mecanismos de seguridad en su desarrollo y mantenimiento.
	Usuarios:



<b>(Nombre del Usuario 1*)</b>	Mtra. Verónica Luna de la Luz
<b>Cargo*:</b>	Subdirectora de Innovación Educativa (CUAIEED)
<b>Funciones*:</b>	Verificar el funcionamiento del sistema y dar apoyo a los docentes y alumnos en el registro.
<b>Obligaciones*:</b>	Cumplir con la obligación legal de resguardar los datos personales.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección de Desarrollo de Sistemas para la Educación	
<b>Identificador único*</b>	CUAIEED-DDSE-08
<b>(Nombre del sistema A1*)</b>	DespegApp
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos
<b>Características del lugar donde se resguardan los soportes: *</b>	Centro de Datos de la CUAIEED, sobre máquinas virtuales. El centro con temperatura controlada y acceso mediante un sistema biométrico.

## 3. ANÁLISIS DE RIESGOS

Dirección de Desarrollo de Sistemas para la Educación	
<b>Identificador único*</b>	CUAIEED-DDSE-08
<b>(Nombre del sistema A1*)</b>	DespegApp

Riesgo*	Impacto*	Mitigación*
Ataques de SQL-Injection	Alto	Actualización de la base de datos y verificación del código utilizado.
Robo de identidad	Medio	Documento de recomendaciones sobre el robo de identidad y cómo evitarlo.  Asignar contraseñas complicadas.  Implementar autenticación de dos pasos.
Vulnerabilidades propias del lenguaje/framework utilizado para el desarrollo de la aplicación	Medio	Actualización a versiones recientes/estables del lenguaje/framework. Mantenimiento continuo al código de la aplicación

#### 4. ANÁLISIS DE BRECHA

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-08	
(Nombre del sistema A1) *	DespegApp	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Actualización de las librerías de seguridad del servidor.	Tras la liberación de algún parche, implementar los parches correspondientes inmediatamente tras una verificación de compatibilidad con la aplicación	Reducir los tiempos para mantener la aplicación actualizada.

Mantener la base de datos de la aplicación actualizada.	Actualización periódica, cada 6 meses, de la base de datos.	Reducir los tiempos para mantener la aplicación actualizada.
Revisar accesos sobre los puertos del servidor.	Solo permitir la conexión a los puertos que se usan para la aplicación.	Actualizar la configuración de seguridad en los puertos del servidor.

## 5. PLAN DE TRABAJO

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-08		
(Nombre del sistema A1) *	DespegApp		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización del lenguaje de programación o framework	<p>Actualizar el lenguaje/framework de desarrollo de la aplicación y sus dependencias</p> <p>Realizar exhaustivas pruebas de funcionalidad en busca de errores o problemas de compatibilidad de las dependencias</p> <p>Verificar el correcto funcionamiento</p> <p>Aplicar las actualizaciones en el servidor de producción</p>	6 meses	Total

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único*</b>	<b>CUAIEED-DDSE-08</b>
<b>(Nombre del sistema A1) *</b>	<b>DespegApp</b>
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
<b>Transferencias mediante el traslado de soportes físicos:</b>	No aplica.
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No aplica.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No aplica.

## **I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

DespegApp no realiza tratamiento de datos personas es soportes físicos, ya que se encuentra en medio electrónico por medio de una base de datos.

## **II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Uso de los archivos log del servidor y la aplicación.

## **III. REGISTRO DE INCIDENTES:**

La aplicación DespegApp se encuentra en fase de pilotaje.

## **V. ACCESO A LAS INSTALACIONES**

<p>1. Seguridad perimetral exterior (las instalaciones del área universitaria)</p> <p>El acceso a la coordinación es mediante un puesto de control en la entrada principal y única, custodiada por personal de seguridad, el cual, solicita una credencial oficial vigente y un registro con el nombre completo, área o persona a la que visita, hora de entrada. El personal de seguridad intercambia la credencial oficial del visitante por un pase de visitante, la cual está numerada por un identificador y un color del área el cual visita. La credencial oficial se queda con el personal de seguridad hasta que el visitante devuelve el pase de acceso y anote la hora de salida. Alrededor de la coordinación se cuenta con cámaras de seguridad ubicadas estratégicamente que graban en tiempo real las 24 horas del día, la entrada principal, entrada a las diferentes áreas, así como los pasillos más transitados.</p>
<p>2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para</p>

soportes electrónicos).

La aplicación DespegApp se encuentra dentro de un servidor que está dentro del centro de datos de la coordinación. El centro de datos se encuentra la planta baja, solo cuenta con una puerta de acceso que sirve de entrada y salida, el acceso está controlado y restringido por un sistema de ingreso con tres formas de acceso:

Un sistema biométrico: el uso de una huella dactilar (dedo índice).

Una clave: clave de 6 dígitos (una clave para cada usuario con acceso).

Una tarjeta de contacto: Tarjeta maestra que da acceso al contacto (Resguardada bajo llave en posesión de los administradores).

Al ingresar al centro de datos con alguna de las tres formas de acceso, el sistema toma una fotografía del usuario que ingresó y emite una alerta sobre el acceso, tanto si el ingreso fue válido o no.

El sistema de ingreso guarda toda la información del acceso o intento de acceso en un sistema de bitácoras que indica: fecha, hora de ingreso, nombre del usuario, número de identificador único, tipo de acceso, si fue entrada o salida del centro de datos y si el acceso fue válido o no.

Así mismo existe una cámara de seguridad grabando las 24 horas y en tiempo real el centro de datos.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

Para la actualización de los datos en la aplicación de DespegApp solo se actualizan a petición de los usuarios que utilizan la aplicación y el encargado de realizar los cambios es el Departamento de Desarrollo de Ecosistemas Educativos.

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

El modelo de control de acceso a la aplicación se encuentra basado en roles (perfiles). El sistema operativo donde se hospeda la aplicación utiliza un sistema de cuentas de usuario local que cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible. La aplicación cifra las contraseñas de los usuarios creados. Los nuevos usuarios son dados de alta por medio de una petición, realizada por los usuarios operativos y es enviada por correo electrónico o chat, el encargado de dar de alta y dar el visto bueno es el Departamento de Desarrollo de Ecosistemas Educativos. Los usuarios trabajan con el sistema mediante una vista web por lo que no requieren de acceso al sistema operativo donde vive la aplicación. El mantenimiento se realiza mediante el acceso al servidor utilizando un mecanismo de llave pública/privada. La protección contra los accesos no autorizados se realiza mediante el filtrado de puertos y el sistema antes mencionado de llaves públicas y privadas en donde el servidor no acepta accesos mediante contraseña.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

La aplicación es respaldada utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello por un promedio de treinta días tras lo cual, es almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas en condiciones óptimas para su funcionamiento. Su resguardo de estas cintas magnéticas es indefinido.

## **IX. PLAN DE CONTINGENCIA**

Para asegurar la continuidad de la aplicación se utiliza como fuente de recuperación los respaldos obtenidos de la aplicación en cintas magnéticas y en un servidor dedicado. El funcionamiento total de la plataforma se garantiza en un tiempo máximo de 12 horas. No se cuenta con un sitio redundante o alterno.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-08	
(Nombre del sistema A1) *	DespegApp	
Recurso*	Descripción*	Control*
Bitácora del sistema	Revisión aleatoria	Revisar de manera aleatoria la bitácora con el fin de identificar algún comportamiento inusual en la aplicación

### 7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-08	
(Nombre del sistema A1) *	DespegApp	
Medida de seguridad*	Procedimiento*	Responsable*
Respaldos de información	Revisión y validación del	Departamento de Operaciones y

	historial de respaldos de la aplicación	Seguridad Informática
Aplicar actualizaciones de seguridad más recientes disponibles	Revisión y actualizaciones del sistema operativo	Departamento de Operaciones y Seguridad Informática

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-08	
(Nombre del sistema A1) *	DespegApp	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Respaldos de información	Se cuenta con respaldos actualizados de la información de la aplicación.	Departamento de Operaciones y Seguridad Informática
Aplicar actualizaciones de seguridad más recientes disponibles	El sistema operativo cuenta con las actualizaciones de seguridad más recientes	Departamento de Operaciones y Seguridad Informática

### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-08

(Nombre del sistema A1) *	DespegApp	
Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL	Renovación anual del certificado SSL para el subdominio donde se encuentra la aplicación	Departamento de Operaciones y Seguridad Informática
Actualización del lenguaje de programación	Actualizar el lenguaje de programación a la próxima versión estable	Departamento de Desarrollo de Ecosistemas Educativos

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

<b>Dirección de Desarrollo de Sistemas para la Educación</b>			
Identificador único*	CUAIEED-DDSE-08		
(Nombre del sistema A1) *	DespegApp		
Actividad*	Descripción*	Duración*	Cobertura*
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Inicio: 19 de abril 2021 Término: 23 de mayo de 2021	Responsables de TI de las dependencias de la UNAM.

### 8.2. Programa de difusión de la protección a los datos personales

<b>No se cuenta con un programa de difusión</b>
---



## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-08		
(Nombre del sistema A1) *	DespegApp		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización de tecnologías de desarrollo	Actualizar el framework de desarrollo de la aplicación y sus dependencias  Realizar exhaustivas pruebas de funcionalidad en busca de errores o problemas de compatibilidad de las dependencias  Verificar el correcto funcionamiento  Aplicar las actualizaciones en el servidor de producción	2 meses	Total

### 9.2. Actualización y mantenimiento de equipo de cómputo

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-08
(Nombre del sistema A1) *	DespegApp

<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
Adquisición de equipo de cómputo para desarrollo de software	Solicitud de compra de nuevo equipo de cómputo para desarrollo de software	5 años	Total

### 9.3. Procesos para la conservación, preservación y respaldos de información

<b>Dirección de Desarrollo de Sistemas para la Educación</b>		
<b>Identificador único*</b>	<b>CUAIEED-DDSE-08</b>	
<b>(Nombre del sistema A1) *</b>	<b>DespegApp</b>	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
Ejecución del script en el servidor de respaldos	El script se conecta al servidor de producción donde está hospedada la aplicación Se realiza la sincronización sobre la carpeta donde se encuentra el código Se realiza una copia de la base de datos Se guardan los datos en el servidor de respaldos	Departamento de Operaciones y Seguridad Informática.  Tiempo: 1 día

### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-08	
(Nombre del sistema A1) *	DespegApp	
Proceso*	Descripción*	Responsable*
Borrado seguro.	Se realiza un formato de bajo nivel al disco duro físico del hipervisor.	Departamento de Operaciones y Seguridad Informática.  Tiempo máximo de 24 horas.

## Moodle

### Introducción

Es una aplicación de software libre que se distribuye bajo la licencia GLP (General Public License). Este sistema de gestión de aprendizaje (LMS), desarrollado en PHP y que utiliza bases de datos MySQL, PostgreSQL o MSSQL.

Las plataformas MOODLE se utilizan para crear cursos y talleres en formato híbrido, mixto y totalmente en línea a nivel bachillerato, licenciaturas, posgrado y doctorado. Estas plataformas se encuentran alojadas en los servidores de la CUAIEED. El acceso a las plataformas a nivel administrador es mediante la creación de usuarios por parte del encargado de la plataforma. Y para los usuarios puede ser manualmente o mediante un proceso de auto registro en el cual se solicita un usuario (identificador único dentro de la plataforma), una contraseña (asignada por el usuario), un correo electrónico, nombres y apellidos.

## 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-09
(Nombre del sistema) *	MOODLE
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, teléfono celular, correo electrónico, RFC, CURP, fecha de nacimiento, nacionalidad, edad, fotografía, idioma o lengua, correo electrónico institucional

<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED)
<b>Nombre*:</b>	Mtro. Ricardo Arroyo Mendoza
<b>Cargo*:</b>	Dirección de Desarrollo de Sistemas para la Educación
<b>Funciones*:</b>	Encargado de gestionar la instalación de la plataforma en las diferentes entidades de la UNAM
<b>Obligaciones*:</b>	Decidir los usuarios y encargados que tendrán accesos administrativos de la plataforma. Vigilar que el sistema cumpla con las medidas de seguridad técnica, físicas y administrativas.
	<b>Encargados:</b>
<b>(Nombre del Encargado 1*)</b>	Mtro. Dulce Campos del Razo
<b>Cargo*:</b>	Subdirección de Informática y Proyectos de Tecnologías de la Información
<b>Funciones*:</b>	Gestión de acceso, planificación, actualización, seguridad y operación continua del sistema y los datos almacenados
<b>Obligaciones*:</b>	Cuidado de los datos personales Conservación de los datos personales Aseguramiento de los datos personales
<b>(Nombre del Encargado 1*)</b>	Mtro. Enrique Tezozomoc Pérez Campos
<b>Cargo*:</b>	Jefe de departamento de operación y seguridad informática
<b>Funciones*:</b>	Gestión de acceso, planificación, actualización, seguridad y operación continua del sistema y los datos almacenados
<b>Obligaciones*:</b>	Cuidado de los datos personales Conservación de los datos personales Aseguramiento de los datos personales
<b>(Nombre del Encargado 1*)</b>	Mtro. Alan López de Jesús
<b>Cargo*:</b>	Jefe de área de operación y seguridad informática
<b>Funciones*:</b>	Gestión de acceso, planificación, actualización, seguridad y operación continua del sistema y los datos almacenados
<b>Obligaciones*:</b>	Cuidado de los datos personales Conservación de los datos personales Aseguramiento de los datos personales

	<b>Usuarios:</b>
<b>(Nombre del Usuario 1*)</b>	Encargado de TI de la Escuela, Facultad, Entidad o Coordinación
<b>Cargo*:</b>	Encargado de TI
<b>Funciones*:</b>	Decidir qué datos personales se solicitan a los usuarios Decidir cuánto tiempo se mantienen los datos personales en el sistema Actualización de los datos dentro del sistema
<b>Obligaciones*:</b>	Cuidado de los datos personales Conservación de los datos personales Aseguramiento de los datos personales

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único**</b>	CUAIEED-DDSE-09
<b>(Nombre del sistema *)</b>	MOODLE
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Sistema de Gestión del Aprendizaje (LMS)
<b>Características del lugar donde se resguardan los soportes: *</b>	Alojamiento en el centro de datos de CUAIEED dentro de diversas máquinas virtuales, este centro de datos cuenta con temperatura controlada y acceso mediante un sistema biométrico.

## 3. ANÁLISIS DE RIESGOS

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único*</b>	CUAIEED-DDSE-09
<b>(Nombre del sistema) *</b>	MOODLE

Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado a la plataforma	Alto	Accesos restringidos mediante el uso de contraseñas seguras (longitud mínima de 10, usando por lo menos, una letra mayúscula, una minúscula, 1 dígito y un carácter especial). Cifrado de comunicaciones entre el cliente y el servidor.
Explotación de vulnerabilidades del propio sistema	Medio	Control de instalación del sistema en versiones estables y actualización de parches de seguridad.
Plugins de terceros	Medio	Actualización de los plugins de terceros y desactivación de plugins no esenciales para el funcionamiento de la plataforma.

#### 4. ANÁLISIS DE BRECHA

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-09	
Nombre del sistema)*	MOODLE	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Cifrado de comunicaciones entre cliente y servidor.	Uso de certificado de seguridad SSL/TLS en todas las comunicaciones realizadas por la plataforma.	Uso en local de imágenes y scripts de javascript para la vista web.

Contraseñas seguras de usuario.	Las contraseñas de usuario deben ser únicas y rotadas constantemente para evitar el descubrimiento por medio de ataques de diccionario.	Cambio de contraseñas de usuario cada seis meses.
Actualización de la plataforma.	Tras liberarse la actualización de la plataforma MOODLE se deben de implementar estos cambios inmediatamente.	Reducir los tiempos requeridos para mantener la plataforma actualizada.

## 5. PLAN DE TRABAJO

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-09		
(Nombre del sistema) *	MOODLE		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización e instalación de parches de seguridad de los sistemas MOODLE	Actualización de plataformas MOODLE en sus versiones estables y con los parches de seguridad	2 horas	Total
Bitácoras de control de roles en las plataformas MOODLE	Realizar una bitácora con los nombres de usuarios que ingresan a las plataformas con perfil de administrador	20 horas	Total
Actualización de datos personales de usuarios.	Los dueños de los datos personales deben de actualizar sus datos personales contenidos dentro de la plataforma para validar que se cuenta	1 días	Parcial

con la información  
actualizada.

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-09
(Nombre del sistema) *	MOODLE
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
Transferencias mediante el traslado de soportes físicos:	No se realiza el traslado de soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realiza el traslado de soportes electrónicos
Transferencias mediante el traslado sobre redes electrónicas:	No se realiza el traslado sobre redes electrónicas

### II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Las plataformas MOODLE no realizan tratamiento de datos personales con soporte físico.

### III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras de las plataformas MOODLE se almacenan en dos lugares:

Uno dentro en formato de log dentro del servidor y otro dentro del propio sistema, que contiene un sistema de bitácoras, en estos se almacena el nombre de usuario, correo e IP desde donde se conectan los usuarios. Los archivos de log que se encuentran dentro del sistema operativo se rotan cada diez días mientras que las bitácoras dentro del propio sistema se almacenan de forma indeterminada hasta el final de la vida útil del sistema. La integridad de las bitácoras se garantiza utilizando una suma de HASH. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática, las herramientas utilizadas para el análisis son AWK, SED y GREP. Solo



los responsables y usuarios con privilegios de administrador pueden ingresar a revisar las bitácoras, en caso de que llegue alguna alerta sobre

#### IV. REGISTRO DE INCIDENTES:

Para las plataformas MOODLE, los incidentes son reportados al Departamento de Operaciones y Seguridad Informática en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuentan con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

El tipo de soporte es electrónico por lo que la recuperación de la base de datos, la cual se encarga de almacenar los datos personales de los usuarios, es el proceso más importante. Este consiste en recuperar el código fuente del sistema de MOODLE, la carpeta de persistencia de los datos y una copia de la base de datos obtenida en el proceso de respaldo programado

Tras realizar la recuperación de los datos se realiza una comparación con un respaldo de la base de datos antes de ser comprometida para validar su estado y determinar la pertinencia de su uso. Si fue utilizado un respaldo para la recuperación se valida su integridad con una suma de HASH. La recuperación de datos es autorizada por el director de la Dirección de Sistemas Educativos para la Educación.

El incidente se registra en un documento, en el cual, se da a conocer la siguiente información:

Nombre del o las personas que registraron el incidente

Nombre del o las personas que soluciona el incidente

Daño causado al sistema

Acciones realizadas para asegurar la integridad de los datos

Tiempo de recuperación de la incidencia

Medidas para evitar el incidente a futuro

#### V. ACCESO A LAS INSTALACIONES

##### Seguridad perimetral exterior

El acceso a la coordinación es mediante un puesto de control en la entrada principal y única, custodiada por personal de seguridad, el cual, solicita una credencial oficial vigente y un registro con el nombre completo, área o persona a la que visita, hora de entrada. El personal de seguridad intercambia la credencial oficial del visitante por un pase de visitante, la cual está numerada por un identificador y un color del área el cual visita. La credencial oficial se queda con el personal de seguridad hasta que el visitante devuelve el pase de acceso y anote la hora de salida.

Alrededor de la coordinación se cuenta con cámaras de seguridad ubicadas estratégicamente que graban en tiempo real las 24 horas del día, la entrada principal, entrada a las diferentes áreas, así como los pasillos más transitados.

##### Seguridad perimetral interior

Las plataformas MOODLE se encuentran dentro de servidores, los cuales, a su vez están dentro del centro de datos de la coordinación. El centro de datos se encuentra la planta baja, solo cuenta con una puerta de acceso que sirve de entrada y salida, el acceso está controlado y restringido por un sistema de ingreso con tres formas de acceso:

Un sistema biométrico: el uso de una huella dactilar (dedo índice)

Una clave: clave de 6 dígitos (una clave para cada usuario con acceso)

Una tarjeta de contacto: Tarjeta maestra que al contacto da acceso (Resguardada bajo llave en posesión de los administradores)

Al ingresar al centro de datos con alguna de las tres formas de acceso, el sistema toma una fotografía del usuario que ingresó y emite una alerta sobre el acceso, tanto si el ingreso fue válido o no. El sistema de ingreso guarda toda la información del acceso o intento de acceso en un sistema de bitácoras que indica: fecha, hora de ingreso, nombre del usuario, número de identificador único, tipo de acceso, si fue entrada o salida del centro de datos y si el acceso fue válido o no. Así mismo existe una cámara de seguridad grabando las 24 horas y en tiempo real el centro de datos.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

Para la actualización de los datos en la plataforma MOODLE solo se actualizan en dos casos:

El mismo dueño de los datos puede modificar sus datos accediendo a la plataforma con su usuario y contraseña.

Los usuarios del sistema con rol de administradores pueden modificar los datos a petición de los propios dueños.

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). El sistema operativo donde se hospedan las aplicaciones utiliza un sistema de cuentas de usuario local que cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible. Las plataformas MOODLE cifran las contraseñas de los usuarios dados de alta en el mismo utilizando MD5 y tiene un manejo estricto de los roles base con los cuales trabaja. Los nuevos usuarios son creados a partir de la petición de usuarios con permisos de administrador o mediante un proceso de inscripción automatizado, la creación de nuevos perfiles de usuario está en manos de los administradores de la plataforma en donde la autorización para su creación es otorgada por el administrador de esta. El departamento de Operaciones y Seguridad Informática lleva el control de los usuarios con permisos de administrador y la creación de nuevos perfiles dentro de la plataforma.

Los usuarios trabajan con el sistema mediante una vista web por lo que no requieren de acceso al sistema operativo donde vive la aplicación. Las tareas de mantenimiento de la plataforma son realizadas mediante el acceso al servidor utilizando un mecanismo de llave pública/privada, solamente los administradores de la plataforma pueden realizar este proceso. La protección contra los accesos no autorizados se realiza mediante el filtrado de puertos y el sistema antes mencionado de llaves públicas y privadas en donde el servidor no acepta accesos mediante contraseña.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

Las plataformas son respaldadas utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello por un promedio de treinta días tras lo cual, es almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas en condiciones óptimas para su funcionamiento. Su resguardo de estas cintas magnéticas es indefinido.

## **IX. PLAN DE CONTINGENCIA**

En caso de desastre se tiene un plan de contingencia el cual garantiza la operación del sistema, esto mediante la realización de espejos en las bases de datos, así como datos persistentes de las plataformas MOODLE, las cuales se encuentran en sincronización para evitar la pérdida de información y convertirse

en producción. Se han realizado pruebas en el cual se ha logrado desplegar el plan de contingencia con una alta velocidad de continuidad del servicio. El plan cuenta con varios sitios espejo que ayudan a mantener la redundancia en caliente. Una vez que se tiene conocimiento de la problemática los encargados de las plataformas acceden a realizar el cambio de dominio, configuración y conexión a los nuevos datos para el despliegue, logrando que el sistema se de alta en un promedio de 5 horas.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-09	
Nombre del sistema*	MOODLE	
Recurso*	Descripción*	Control*
Gestor de usuarios del sistema	La plataforma MOODLE cuenta con un gestor de usuarios que muestra la fecha en la que el usuario ingresó por primera y última vez	Solo los usuarios administradores se les da el acceso para revisar y monitorear el gestor de usuarios
Nagios	Sistema de monitorización de redes, que vigila el estado y servicios dentro del equipo de la plataforma MOODLE, alertando cuando el comportamiento de estos se detecten intrusiones o procesos anormales	Solo los administradores tienen acceso al sistema de monitoreo Nagios mediante acceso restringido.  Sistema de software abierto con Licencia GPLv2
Top	El comando top proporciona una vista dinámica en tiempo real de un sistema en ejecución. Puede mostrar información de resumen del sistema, así como una lista de tareas que actualmente administra el kernel de Linux.	Este comando de monitoreo solo puede ser utilizado por los administradores del servidor donde está la plataforma MOODLE con acceso restringido

### 7.2. Procedimiento para la revisión de las medidas de seguridad

**Dirección de Desarrollo de Sistemas para la Educación**

<b>Identificador único*</b>	CUAIEED-DDSE-09	
<b>Nombre del sistema)*</b>	MOODLE	
<b>Medida de seguridad*</b>	<b>Procedimiento*</b>	<b>Responsable*</b>
Revisión de permisos.	Revisiones de permisos dentro del servidor web y la aplicación.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de dos horas.
Script de respaldos de información.	Revisión aleatoria del contenido de los respaldos realizados.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización del sistema operativo.	Actualización a nuevas versiones de los paquetes del sistema operativo.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización de la aplicación.	Actualización de plugins y componentes principales del núcleo de MOODLE.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Revisión de permisos.	Revisiones de permisos dentro del servidor web y la aplicación.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de dos horas.

**7.3. Resultados de la evaluación y pruebas a las medidas de seguridad**

**Dirección de Desarrollo de Sistemas para la Educación**

Identificador único*	CUAIEED-DDSE-09	
Nombre del sistema) *	MOODLE	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Revisión de permisos.	Se cuentan con los permisos adecuados.	Responsable: Departamento de Operaciones y Seguridad Informática.
Script de respaldos de información.	Los respaldos funcionan correctamente.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización del sistema operativo.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización de la aplicación.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.

#### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

<b>Dirección de Desarrollo de Sistemas para la Educación</b>		
Identificador único*	CUAIEED-DDSE-09	
Nombre del sistema) *	MOODLE	
Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL.	Realizar la renovación anual del certificado SSL.	Responsable: Dirección de Sistemas para la Educación.

Actualización de la plataforma Moodle	Realizar el proceso de actualización de la plataforma	Responsable: Departamento de Operaciones y Seguridad Informática
---------------------------------------	---	--

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-09		
(Nombre del sistema) *	MOODLE		
Actividad*	Descripción*	Duración*	Cobertura*
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Inicio: 19 de abril 2021 Término: 23 de mayo de 2021	Responsables de TI de las dependencias de la UNAM.

### 8.2. Programa de difusión de la protección a los datos personales

No se cuenta con un programa de difusión
--

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

Dirección de Desarrollo de Sistemas para la Educación
---

<b>Identificador único*</b>	CUAIEED-DDSE-09		
<b>(Nombre del sistema) *</b>	MOODLE		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
<i>Actualización de la plataforma MOODLE a nuevas versiones.</i>	<i>Proceso de actualización hacia versiones superiores de la plataforma MOODLE.</i>	<i>1 mes.</i>	<i>Total.</i>

## 9.2. Actualización y mantenimiento de equipo de cómputo

<b>Dirección de Desarrollo de Sistemas para la Educación</b>			
<b>Identificador único*</b>	CUAIEED-DDSE-09		
<b>(Nombre del sistema) *</b>	MOODLE		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
<i>Actualización del servidor físico.</i>	<i>Cambio del servidor físico utilizado para crear máquinas virtuales donde se hospedan las aplicaciones MOODLE.</i>	<i>3 años</i>	<i>Total.</i>

## 9.3. Procesos para la conservación, preservación y respaldos de información

<b>Dirección de Desarrollo de Sistemas para la Educación</b>
--

<b>Identificador único*</b>	CUAIEED-DDSE-09	
<b>(Nombre del sistema) *</b>	MOODLE	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
<i>Resguardo de cintas magnéticas.</i>	<i>Las cintas magnéticas realizadas en la fase de respaldo automatizado son resguardadas de forma indefinida en un almacén.</i>	<i>Departamento de Operaciones y Seguridad Informática.</i>

#### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección de Desarrollo de Sistemas para la Educación		
<b>Identificador único*</b>	CUAIEED-DDSE-09	
<b>(Nombre del sistema) *</b>	MOODLE	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
<i>Borrado seguro.</i>	<i>Se realiza un formato de bajo nivel al disco duro físico del hipervisor.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.</i>

### Drupal

#### Introducción

La plataforma CMS Drupal se utiliza como un gestor de contenidos que permite la creación de sitios web dinámicos y estáticos utilizado en la Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia para crear y distribuir contenido educativo creado por las diversas entidades del SUAyED. En esta plataforma se almacenan datos personales de usuarios de diversas entidades que tienen acceso a los contenidos los cuales son gestionados por un administrador de plataforma.

#### 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES



<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único*</b>	CUAIEED-DDSE-10
<b>Nombre del sistema A1*:</b>	<b>Drupal</b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre, correo electrónico (personal o institucional), institución de procedencia.
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
<b>Nombre*:</b>	Mtro. Ricardo Arroyo Mendoza
<b>Cargo*:</b>	Director de Desarrollo de Sistemas para la Educación
<b>Funciones*:</b>	Definir la arquitectura tecnológica necesaria para el funcionamiento y mantenimiento de la infraestructura y las plataformas de la Coordinación.
<b>Obligaciones*:</b>	<ul style="list-style-type: none"> <li>- Definir junto con los usuarios del sistema, los tipos de acceso.</li> <li>- Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.</li> </ul>
	<b>Encargados:</b>
<b>(Nombre del Encargado 1*:</b>	Mtro. Alan López de Jesús
<b>Cargo*:</b>	Jefe de Área del Departamento de Operaciones y Seguridad Informática.
<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 2*:</b>	Mtro. Enrique Tezozomoc Pérez Campos
<b>Cargo*:</b>	Jefe del Departamento de Operaciones y Seguridad Informática
<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual

	de los sistemas o servidores de la Coordinación.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 3*:</b>	Mtra. Edith Tapia Rangel
<b>Cargo*:</b>	Subdirectora de Proyectos de Educación Abierta y a Distancia
<b>Funciones*:</b>	Realizar el diseño de sitios web dinámicos y estáticos diseñados para atender las distintas necesidades de los proyectos de la institución.
<b>Obligaciones*:</b>	Procurar la protección de los datos personales contenidos en el sistema.
	<b>Usuarios:</b>
<b>(Nombre del Usuario *)</b>	Entidades y Facultades pertenecientes a la UNAM.
<b>Cargo*:</b>	Comunidad académica, estudiantil y funcionarios
<b>Funciones*:</b>	Consultar el contenido de los sitios a los cuales tiene acceso y gestionar la información perteneciente a su Entidad o Facultad.
<b>Obligaciones*:</b>	Validar que la información que se distribuye dentro del sistema no contenga datos personales visibles de la comunidad universitaria o un tercero.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección de Desarrollo de Sistemas para la Educación</b>	
<b>Identificador único**</b>	CUAIEED-DDSE-10
<b>(Nombre del sistema *)</b>	Drupal
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos
<b>Características del lugar donde se resguardan los soportes: *</b>	Almacenamiento en el centro de datos de CUAIEED dentro de diversas máquinas virtuales, el cual cuenta con acceso mediante un sistema

### 3. ANÁLISIS DE RIESGOS

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-10	
Nombre del sistema)*	Drupal	
Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado.	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor.
Explotación de vulnerabilidades.	Medio	Actualización del core de CMS Drupal.
Plugins de terceros.	Medio	Actualización de los plugins de terceros y desactivación de plugins no esenciales para el funcionamiento de la plataforma.

### 4. ANÁLISIS DE BRECHA

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-10
Nombre del sistema)*	Drupal

Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Cifrado de comunicaciones entre cliente y servidor.	Uso de certificado de seguridad SSL/TLS en todas las comunicaciones realizadas por la plataforma.	Uso en local de imágenes y javascript obtenidos de terceros por el CMS Drupal para la vista web.
Contraseñas seguras de usuario.	Las contraseñas de usuario deben ser únicas y rotadas constantemente para evitar el descubrimiento por medio de ataques de diccionario.	Cambio de contraseñas de usuario cada seis meses.
Actualización de la plataforma.	Tras liberarse la actualización de la plataforma Drupal se deben de implementar estos cambios inmediatamente.	Reducir los tiempos requeridos para mantener la plataforma actualizada.

## 5. PLAN DE TRABAJO




## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-10
(Nombre del sistema) *	Drupal
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
<b>Transferencias mediante el traslado de soportes físicos:</b>	No se realiza tratamiento de datos personales con soportes físicos, se tiene soporte electrónico en una base de datos.
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias mediante el traslado de soportes electrónicos.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No se realizan transferencias mediante el traslado sobre redes electrónicas.

### I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No aplica, se tiene soporte electrónico en una base de datos.

### II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web y la base de datos del CMS Drupal, almacenando la fecha, hora, dirección IP, así como todas las acciones dentro del sistema. Los archivos de log que se encuentran dentro del sistema operativo se rotan cada determinado día mientras que las bitácoras dentro de la base de datos se almacenan de forma indeterminada hasta el final de la vida útil del sistema. La integridad de las bitácoras se garantiza utilizando una suma de HASH. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática, las herramientas utilizadas para el análisis son AWK, SED y GREP.

### III. REGISTRO DE INCIDENTES

Los incidentes son reportados al Departamento de Operaciones y Seguridad Informática en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuenta con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

El tipo de soporte es electrónico por lo que la recuperación de la base de datos, la cual se encarga de almacenar los datos personales de los usuarios, es el proceso más importante. Este consiste en recuperar el código fuente del CMS Drupal junto con una copia de la base de datos obtenida en el proceso de respaldo programado.

Tras realizar la recuperación de los datos se realiza una comparación con un respaldo de la base de datos antes de ser comprometida para validar su estado y determinar la pertinencia de su uso. Si fue utilizado un respaldo para la recuperación se valida su integridad con una suma de HASH. La recuperación de datos es autorizada por el responsable del sistema.

## V. ACCESO A LAS INSTALACIONES

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente. La dependencia se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el director de la Dirección de Desarrollo de Sistemas para la Educación.

## VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales se encuentra indicado dentro de la plataforma, información disponible únicamente para usuarios registrados, y el cual consiste en que el solicitante de una corrección de datos personales deberá de enviar un ticket a la mesa de ayuda de la plataforma en donde, tras identificarse como usuario de la plataforma con su ID único, indicará el dato incorrecto, la plataforma y los nuevos datos a actualizar. El cambio se realizará en un plazo no mayor a cuarenta y ocho horas tras ser recibida la solicitud en horario y días laborables.

## VII. PERFILES DE USUARIO Y CONTRASEÑAS

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). El sistema operativo, donde se hospedan las aplicaciones, utiliza un sistema de cuentas de usuario local que cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible. El CMS Drupal cifra las contraseñas de los usuarios dados de alta en el mismo utilizando MD5 y tiene un manejo estricto de los roles base con los cuales trabaja. Los nuevos usuarios son creados a partir de la petición de usuarios con permisos de administrador o mediante un proceso de inscripción automatizado, la creación de nuevos perfiles de usuario está en manos de los administradores de la plataforma en donde la autorización para su creación es otorgada por el administrador de esta. El departamento de Operaciones y Seguridad Informática lleva el control de los usuarios con permisos de administrador y la creación de nuevos perfiles dentro de la plataforma.

Los usuarios trabajan con el sistema mediante una vista web, por lo que no requieren de acceso al sistema operativo donde se aloja la aplicación. Las tareas de mantenimiento de la plataforma son realizadas mediante el acceso al servidor utilizando un mecanismo de llave pública/privada, solamente los administradores de la plataforma pueden realizar este proceso. La protección contra los accesos no autorizados se realiza mediante el filtrado de puertos y el sistema antes mencionado de llaves públicas y privadas en donde el servidor no acepta accesos mediante contraseña.

**VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

Las plataformas son respaldadas utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello, por un promedio de treinta días tras, y almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas seguras y en condiciones óptimas para su funcionamiento. Para promover la conservación y preservación de la información, las cintas y el lector de estas se mantienen por tiempo indefinido.

**IX. PLAN DE CONTINGENCIA**

Se cuenta con un plan de contingencia que permite la continuidad de negocio, el cual utiliza como fuente primordial los respaldos obtenidos de las plataformas en cintas magnéticas y en un servidor dedicado. Las pruebas de eficiencia que se realizan han garantizado la recuperación total de la plataforma en un periodo máximo de doce horas. Actualmente no se cuenta con un sitio redundante o alterno.

**7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD**

**7.1. Herramientas y recursos para monitoreo de la protección de datos personales**

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-10	
Nombre del sistema A1)	Drupal	
Recurso*	Descripción*	Control*
Herramientas automatizadas	Se realiza una inspección de un sistema CMS Drupal, revisión de la configuración de seguridad del servidor web, revisión de permisos de usuarios e integridad de la plataforma.	Las herramientas utilizadas son OpenVas, Owasp Zen Attack Proxy y Vega.  Responsables: Departamento de Operaciones y Seguridad Informática.

Bitácoras del sistema	Revisión aleatoria del contenido de los logs del sistema operativo y aplicación.	Se realiza una revisión no automatizada buscando patrones de ataque conocidos y secuencias de ataques conocidos como el descubrimiento de puertos y búsqueda de archivos de configuración conocidos.  Responsables: Departamento de Operaciones y Seguridad Informática.
-----------------------	--	--

## 7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-10	
Nombre del sistema)*	Drupal	
Medida de seguridad*	Procedimiento*	Responsable*
Revisión de permisos.	Revisión de permisos dentro del servidor web y la aplicación.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de dos horas.
Script de respaldo de información.	Revisión aleatoria del contenido de los respaldos realizados.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización del sistema operativo.	Actualización a nuevas versiones de los paquetes del sistema operativo.	Responsable: Departamento de Operaciones y Seguridad Informática. La duración es de una hora.
Actualización de la aplicación.	Actualización de plugins y componentes principales del núcleo de Drupal.	Responsable: Departamento de Operaciones y Seguridad Informática.



		Informática. La duración es de una hora.
--	--	--

**7.3. Resultados de la evaluación y pruebas a las medidas de seguridad**

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-10	
Nombre del sistema)*	Drupal	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Revisión de permisos.	Se cuentan con los permisos adecuados.	Responsable: Departamento de Operaciones y Seguridad Informática.
Script de respaldos de información.	Los respaldos funcionan correctamente.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización del sistema operativo.	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.
Actualización de la aplicación	Se cuentan con las últimas actualizaciones.	Responsable: Departamento de Operaciones y Seguridad Informática.

**7.4. Acciones para la corrección y actualización de las medidas de seguridad**

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DDSE-10

Nombre del sistema) *	Drupal	
Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL	Realizar la renovación anual del certificado SSL	Responsable: Dirección de Desarrollo de Sistemas para la Educación.
Actualización de la plataforma CMS Drupal	Realizar el proceso de actualización de la plataforma	Responsable: Departamento de Operaciones y Seguridad Informática

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-10		
(Nombre del sistema) *	Drupal		
Actividad*	Descripción*	Duración*	Cobertura*
Medidas de Seguridad Técnicas para la Protección de Datos Personales	Curso en línea	25 horas. Inicio: 19 de abril 2021 Término: 23 de mayo de 2021	Responsables de TI de las dependencias de la UNAM.

### 8.2. Programa de difusión de la protección a los datos personales

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

No se tiene un programa de difusión de la protección a los datos personales

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-10		
(Nombre del sistema) *	Drupal		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización de la plataforma a nuevas versiones.	Proceso de actualización hacia versiones superiores de la plataforma CMS Drupal.	1 mes.	Total.

### 9.2. Actualización y mantenimiento de equipo de cómputo

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DDSE-10		
(Nombre del sistema) *:	Drupal		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización del servidor físico.	Cambio del servidor físico utilizado para crear máquinas virtuales donde se hospedan las aplicaciones CMS Drupal.	3 años.	Total.

### 9.3. Procesos para la conservación, preservación y respaldos de información

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-10	
(Nombre del sistema *:	Drupal	
Proceso*	Descripción*	Responsable*
Resguardo de cintas magnéticas.	Las cintas magnéticas realizadas en la fase de respaldo automatizado son resguardadas de forma indefinida en un almacén.	Departamento de Operaciones y Seguridad Informática.

### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección de Desarrollo de Sistemas para la Educación		
Identificador único*	CUAIEED-DDSE-10	
(Nombre del sistema *:	Drupal	
Proceso*	Descripción*	Responsable*
Borrado seguro.	Se realiza un formato de bajo nivel al disco duro físico del hipervisor. Tiempo máximo de 24 horas.	Responsable: Departamento de Operaciones y Seguridad Informática.

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El director de la Dirección de Desarrollo de Sistemas para la Educación recibe o envía la petición en donde se indica la razón para la cancelación del sistema, el tiempo que deberá de permanecer la plataforma funcionando antes de ser eliminada y si se necesita entregar un respaldo final del sistema

para su resguardo final en un soporte electrónico. La petición siempre es en formato escrito ya sea por correo electrónico o por oficio. El sistema será eliminado tras una fecha de término establecida y se borra de forma permanente la máquina virtual donde este reside.

## **Sistema de Gestión de Formación Docente**

### **Introducción**

El Sistema de Gestión de Formación Docente acompaña y facilita los procesos de administración de actividades académicas durante todo ciclo de vida, desde la creación de las propuestas de actividad hasta la impartición y posterior creación dinámica y almacenamiento de documentos probatorios. El sistema consume web services tanto del sistema de administración de personal de la UNAM como de la Firma Electrónica Universitaria de DGTIC, el primero ofrece la función de validación de usuarios trabajadores en activo y la segunda permite la firma y autenticación de los documentos probatorios que se entregan digitalmente. Cuenta con los módulos Personas, Registro de aspirantes, Captura de propuestas, Eventos, Folios y Documentos probatorios.

### **1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES**

<b>Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente</b>	
<b>Identificador único*</b>	CUAIEED-DIEDCFD-001
<b>Nombre del sistema A1*:</b>	<b>Sistema de Gestión de Formación Docente</b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre, RFC, género, correo electrónico (personal o institucional), número de trabajador, fecha de nacimiento, Tipo de contrato, institución de procedencia, IP
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
<b>Nombre*:</b>	Dra. <a href="#">Ruth Torres Carrasco</a>
<b>Cargo*:</b>	Subdirección del Centro de Formación y Profesionalización para el Desarrollo Académico
<b>Funciones*:</b>	Elaboración de plataformas, materiales y apoyos didácticos multimedia que utilicen la tecnología con enfoques innovadores Elaboración de sistemas académico-administrativos para el apoyo de las actividades de formación docente Impartición de cursos, talleres y diplomados

<b>Obligaciones*:</b>	<ul style="list-style-type: none"> <li>- Definir junto con los usuarios del sistema, los tipos de acceso.</li> <li>- Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.</li> <li>- Vigilar que los sistemas operen de manera adecuado y apegados a su propósito</li> <li>- Vigilar el correcto tratamiento y resguardo de los datos personales almacenados</li> </ul>
	<b>Encargados:</b>
<b>(Nombre del Encargado 1*):</b>	Ing. <a href="#">Carlos Alberto Jaimes Vergara</a>
<b>Cargo*:</b>	Coordinador de Formación Digital y Recursos Audiovisuales para la Docencia
<b>Funciones*:</b>	<p>Asegurar el correcto funcionamiento del sistema, agregar nuevas funcionalidades en una dinámica de mejora continua.</p> <p>Atender necesidades de los usuarios operativos del sistema, programando módulos al sistema y otorgando capacitación sobre ellos.</p>
<b>Obligaciones*:</b>	<p>Proteger el software y la base de datos, así como llevar a cabo los procesos de actualización de la plataforma.</p> <p>Monitorear el comportamiento del sistema</p> <p>Procurar la protección de los datos personales contenidos en el sistema.</p>
<b>(Nombre del Encargado 2*):</b>	<a href="#">Paulina Manjarrez Molina</a>
<b>Cargo*:</b>	Jefa de Departamento de Desarrollo Académico
<b>Funciones*:</b>	Llevar a cabo todos los procesos de generación, gestión, seguimiento de actividades académicas, revisión de requisitos en la participación de usuarios en dichas actividades, así como la elaboración y entrega de documentos probatorios.
<b>Obligaciones*:</b>	<p>Utilizar de manera adecuada y responsable el sistema.</p> <p>Procurar la protección de los datos personales contenidos en el sistema.</p>
<b>(Nombre del Encargado 3*):</b>	Dra. <a href="#">Ruth Torres Carrasco</a>
<b>Cargo*:</b>	Subdirección del Centro de Formación y Profesionalización para el Desarrollo Académico
<b>Funciones*:</b>	Firmar Digitalmente los folios de los participantes con derecho a obtener documentos probatorios

<b>Obligaciones*:</b>	Procurar la protección de los datos personales contenidos en el sistema.
<b>(Nombre del Encargado 4*):</b>	Dr. <a href="#">Melchor Sánchez Mendiola</a>
<b>Cargo*:</b>	Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia
<b>Funciones*:</b>	Firmar Digitalmente los folios de los participantes con derecho a obtener documentos probatorios
<b>Obligaciones*:</b>	Procurar la protección de los datos personales contenidos en el sistema.
<b>(Nombre del Encargado 5*):</b>	Mtra.: Ana María del Pilar Martínez Hernández
<b>Cargo*:</b>	Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente
<b>Funciones*:</b>	Firmar Digitalmente los folios de los participantes con derecho a obtener documentos probatorios
<b>Obligaciones*:</b>	Procurar la protección de los datos personales contenidos en el sistema.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente</b>	
<b>Identificador único*</b>	CUAIEED-DIEDCFD-001
<b>(Nombre del sistema A1*)</b>	<b>Sistema de Gestión de Formación Docente</b>
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Sistema web + web app + Base de datos



### 3. ANÁLISIS DE RIESGOS

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-001	
Nombre del sistema A1) *	Sistema de Gestión de Formación Docente	
Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado.	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor. Cambio de credenciales periódicamente
Acceso Directo a registros de la base de datos	Alto	Cifrado de datos
Explotación de vulnerabilidades.	Medio	Actualización de Marcos de trabajo y plugins terceros
Acceso a registros en el servicio de envío de correos Mailchimp	Bajo	Credenciales robustas y cambio de estas de forma periódica



#### 4. ANÁLISIS DE BRECHA

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-001	
Nombre del sistema A1) *	Sistema de Gestión de Formación Docente	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Acceso a base de datos sólo desde una IP específica dentro del centro de datos y a través de un túnel cifrado con SSH	Registros de datos cifrados	Desarrollo de cifrado de datos desde el sistema
Accesos a través de contraseñas seguras	Adición de JWT (JSON Web Token) para agregar otra capa de seguridad	Implementar sesiones de usuario basadas en tokens web JSON
Utilización del servicio Mailchimp para hacer envíos masivos de correos	Envío de todos los correos de modo independiente y autónomo desde el mismo sistema. De tal modo que se deje de usar Mailchimp	Desarrollar un módulo de envío masivo de correos

#### 5. PLAN DE TRABAJO

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente			
Identificador único*	CUAIEED-DIEDCFD-001		
(Nombre del sistema A1) *	Sistema de Gestión de Formación Docente		
Actividad*	Descripción*	Duración*	Cobertura*

Desarrollo de cifrado de datos desde el sistema	Diseñar e implementar proceso de cifrado y descifrado de todos los datos contenidos en la actual Base de datos, de tal modo que, aunque un usuario malintencionado tuviera acceso a la base, no pueda descifrarlos	3 semanas	Total
Implementar sesiones de usuario basadas en tokens web JSON	Desarrollo de validación de usuarios y consultas a través de sesiones soportadas por JWT	2 semanas	Parcial
Desarrollar un módulo de envío masivo de correos	Diseño e implementación de un módulo completo de envío masivo de correos de tal modo que se evite el uso de un servicio tercero y así disminuir la posible filtración de los datos almacenados en dicho servicio (Mailchimp)	4 semanas	Total

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

<b>Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente</b>	
<b>Identificador único*</b>	CUAIEED-DIEDCFD-001
<b>(Nombre del sistema A1) *</b>	<b>Sistema de Gestión de Formación Docente</b>
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
<b>Transferencias mediante el traslado de soportes físicos:</b>	No se realiza tratamiento de datos personales con soportes físicos, se tiene soporte electrónico en una base de datos.
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias mediante el traslado de soportes electrónicos.
<b>Transferencias mediante el traslado</b>	La transferencia de datos entre sistemas (FEU

<b>sobre redes electrónicas:</b>	DGTIC y DGP) se dan de manera cifrada y la conexión se da de manera exclusiva entre las partes vía whitelist de IP y rutas de acceso y métodos específicos.
----------------------------------	---

## **I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

No aplica, se tiene soporte electrónico en una base de datos.

## **II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web y la base de datos del Sistema de Gestión de Formación Docente, almacenando la fecha, hora, dirección IP, así como todas las acciones dentro del sistema. Los archivos de log que se encuentran dentro del sistema operativo se rotan cada semana.

## **III. REGISTRO DE INCIDENTES**

Los incidentes son reportados a los encargados de infraestructura de la Unidad de Sistemas de la CUAIEED en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuenta con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

La base de datos es respaldada diariamente y son rotadas cada 15 días, por su parte el backend y frontend del aplicativo se encuentra en un repositorio GIT privado y puede ser recuperada cualquier versión del sistema.

## **V. ACCESO A LAS INSTALACIONES**

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente. La dependencia se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar).

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

El procedimiento para actualizar o corregir datos personales se realiza directamente con la encargada del área operativa de Formación Docente, indicando previamente que los datos resguardados son transferidos directamente de los registros de la Dirección General de Personal, por lo que es muy raro que se requieran actualizaciones, sin embargo, las actualizaciones que competan directamente al alcance del sistema se realizarán en un plazo no mayor a cuarenta y ocho horas tras ser recibida la solicitud en horario y días laborables.

## VII. PERFILES DE USUARIO Y CONTRASEÑAS

El número de usuarios del sistema con acceso a datos personales es muy reducido, hasta la elaboración de este documento sólo existen 5 usuarios, 2 con rol de administradores del sistema y 3 con rol de firmantes digitales de documentos probatorios.

Por otro lado, el sistema ofrece el registro a Docentes en activo de la Universidad a las diversas actividades académicas llevadas a cabo por la coordinación y entrega los documentos probatorios firmados digitalmente y autenticados por FEU de la DGTIC.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se cuenta con un esquema de respaldo diario tanto del sistema, la configuración middleware y del servidor, además de la base de datos, con una rotación cada 15 días naturales, además el sistema backend y frontend están resguardados en un repositorio GIT privado.

## IX. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de negocio, el cual utiliza como fuente de datos los últimos respaldos montados en un servidor virtual dedicado. La recuperación total del sistema puede ser llevada en un periodo máximo de 36 horas. Actualmente no se cuenta con un sitio redundante o alterno.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente		
Identificador único	CUAIEED-DIEDCFD-001	
Nombre del sistema A1	Sistema de Gestión de Formación Docente	
Recurso	Descripción	Control
Bitácoras del sistema	Revisión aleatoria del contenido de los logs del sistema operativo y aplicación.	Se realiza una revisión no automatizada buscando patrones de ataque conocidos y secuencias de ataques conocidos como el descubrimiento de puertos y búsqueda de archivos de configuración conocidos.

### 7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-001	
Nombre del sistema A1) *	Sistema de Gestión de Formación Docente	
Medida de seguridad*	Procedimiento*	Responsable*
Script de respaldo de información.	Revisión aleatoria del contenido de los respaldos realizados.	Responsable: Coordinación de formación Digital y Recursos Audiovisuales para la Docencia
Actualización de la aplicación.	Actualización de componentes principales del Sistema de Gestión de Formación Docente.	Responsable: Coordinación de formación Digital y Recursos Audiovisuales para la Docencia

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-001	
Nombre del sistema A1) *	Sistema de Gestión de Formación Docente	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Revisión Cert UNAM	Se cuentan con el aval de DGTIC	Responsable: Coordinación de formación Digital y Recursos Audiovisuales para la Docencia

### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente		
--	--	--

Identificador único*	CUAIEED-DIEDCFD-001	
Nombre del sistema A1) *	Sistema de Gestión de Formación Docente	
Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL.	Realizar la renovación periódica del certificado SSL.	Responsable: Coordinación de formación Digital y Recursos Audiovisuales para la Docencia
Actualización del Sistema de Gestión de Formación Docente.	Realizar el proceso de actualización del sistema.	Responsable: Coordinación de formación Digital y Recursos Audiovisuales para la Docencia

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

No se cuenta con un programa formal de capacitación

### 8.2. Programa de difusión de la protección a los datos personales

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

No se tiene un programa de difusión de la protección a los datos personales

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

<b>Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente</b>	
Identificador único*	CUAIEED-DIEDCFD-001
(Nombre del sistema A1) *	<b>Sistema de Gestión de Formación Docente</b>

Actividad*	Descripción*	Duración*	Cobertura*
<i>Actualización del Sistema de Gestión de Formación Docente.</i>	<i>Realizar el proceso de actualización del sistema.</i>	<i>Periódica.</i>	<i>Parcial e incremental</i>

## 9.2. Actualización y mantenimiento de equipo de cómputo

Dirección de Desarrollo de Sistemas para la Educación			
<b>Identificador único*</b>	CUAIEED-DIEDCFD-001		
<b>(Nombre del sistema A1*:</b>	<b>Sistema de Gestión de Formación Docente</b>		
Actividad*	Descripción*	Duración*	Cobertura*
<i>Actualización del servidor físico.</i>	<i>Cambio del servidor físico utilizado para crear máquinas virtuales donde se hospedan las aplicaciones CMS Sistema de Gestión de Formación Docente.</i>	<i>3 años.</i>	<i>Total.</i>

## 9.3. Procesos para la conservación, preservación y respaldos de información

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente		
<b>Identificador único*</b>	CUAIEED-DIEDCFD-001	
<b>(Nombre del sistema A1*:</b>	<b>Sistema de Gestión de Formación Docente</b>	
Proceso*	Descripción*	Responsable*

<i>Resguardo de cintas magnéticas.</i>	<i>Las cintas magnéticas realizadas en la fase de respaldo automatizado y el lector de las cintas magnéticas son resguardadas de forma indefinida.</i>	<i>Departamento de Operaciones y Seguridad Informática.</i>
--	--	---

#### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

<b>Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente</b>		
<b>Identificador único*</b>	CUAIEED-DIEDCFD-001	
<b>(Nombre del sistema A1*:</b>	<b>Sistema de Gestión de Formación Docente</b>	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
<i>Borrado seguro.</i>	<i>Se realiza un formato de bajo nivel al disco duro físico del hipervisor.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.</i>

### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente recibe o envía la petición en donde se indica la razón para la cancelación del sistema, el tiempo que deberá de permanecer la plataforma funcionando antes de ser eliminada y si se necesita entregar un respaldo final del sistema para su resguardo final en un soporte electrónico. La petición siempre es en formato escrito ya sea por correo electrónico o por oficio. El sistema será eliminado tras una fecha de término establecida y se borra de forma permanente la máquina virtual donde este reside.

#### **Tienda Virtual CUAIEED**

##### **Introducción**

La plataforma de “Tienda Virtual CUAIEED”, es una tienda virtual enfocada a la venta de cursos y servicios de capacitación principalmente del área de educación continua. Tiene la capacidad de realizar cobros por medio de tarjeta de crédito en línea y pagos en ventanilla bancaria, así como la generación y validación de facturas y tickets utilizando servicios web proporcionados por el área del patronato de la UNAM. El sistema Web cuenta con cinco perfiles de usuario: “Administrador del sistema”, “Encargado de tienda”, “Encargado del área administrativa”, “usuario autenticado” y “usuario anónimo”



## 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente</b>	
<b>Identificador único*</b>	CUAIEED-DIEDCFD-002
<b>Nombre del sistema A1*:</b>	<b><u>Tienda Virtual CUAIEED</u></b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	<ul style="list-style-type: none"> <li>● Correo electrónico</li> <li>● Datos para facturación               <ul style="list-style-type: none"> <li>○ RFC</li> <li>○ Nombre / Razón social</li> <li>○ Dirección</li> <li>○ Correo electrónico</li> </ul> </li> </ul>
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
<b>Nombre*:</b>	<b>Mtra. Ana María del Pilar Martínez Hernández</b>
<b>Cargo*:</b>	Directora de Innovación Educativa, Desarrollo Curricular y Formación Docente
<b>Funciones*:</b>	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
<b>Obligaciones*:</b>	<ul style="list-style-type: none"> <li>- Definir junto con los responsables del sistema, los tipos de acceso.</li> <li>- Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.</li> </ul>
<b>Encargados</b>	
<b>(Nombre del Encargado 1*:</b>	<b>Dra. Ruth Torres Carrasco</b>
<b>Cargo*:</b>	Subdirectora Centro de Formación y Profesionalización para el Desarrollo Académico

<b>Funciones*:</b>	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
<b>Obligaciones*:</b>	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>(Nombre del Encargado 2*:</b>	<b>Mtro. Oscar Escamilla González</b>
<b>Cargo*:</b>	Jefe de Departamento de Desarrollos Digitales para la formación Docente
<b>Funciones*:</b>	Desarrollar y dar mantenimiento al sistema, crear respaldo, así como brindar soporte técnico a los usuarios. Administrar la configuración del sitio, crear tiendas, publicar productos.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 3*:</b>	<b>Paulina Manjarrez Molina</b>
<b>Cargo*:</b>	Jefa del Departamento de Educación Continua y Extensión Académica
<b>Funciones*:</b>	Brindar seguimiento a los procesos de registro y compra de usuarios.
<b>Obligaciones*:</b>	Cumplir con la obligación legal de resguardar los datos personales.
<b>(Nombre del Encargado 4*:</b>	<b>Lic. Erick Arturo Hernández Moreno</b>
<b>Cargo*:</b>	Jefe del Departamento de Presupuesto
<b>Funciones*:</b>	<ul style="list-style-type: none"> <li>● Verificar y consolidar pagos.</li> <li>● Gestionar tickets y facturas.</li> </ul>
<b>Obligaciones*:</b>	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)

<b>(Nombre del Encargado 5*:</b>	<b>Ing. Milton Arturo García Lima</b>
<b>Cargo*:</b>	Jefe de la Unidad de Sistemas para la Evaluación Educativa
<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>Usuarios:</b>	
<b>(Nombre del Usuario *)</b>	Público en general
<b>Cargo*:</b>	N/A
<b>Funciones*:</b>	Realizar compras, editar y gestionar sus datos personales en el sistema.
<b>Obligaciones*:</b>	Validar sus compras y gestionar sus datos personales en el sistema.
<b>(Nombre del Usuario 2*)</b>	<b>Lic. Erick Arturo Hernández Moreno</b>
<b>Cargo*:</b>	Jefe del Departamento de Presupuesto
<b>Funciones*:</b>	<ul style="list-style-type: none"> <li>● Verificar y consolidar pagos.</li> <li>● Gestionar tickets y facturas.</li> </ul>
<b>Obligaciones*:</b>	Verificar pagos, facturas y tickets para conciliar información con los sistemas de administración de la entidad.
<b>(Nombre del Usuario 3*)</b>	<b>Paulina Manjarrez Molina</b>
<b>Cargo*:</b>	Jefa del Departamento de Educación Continua y Extensión Académica
<b>Funciones*:</b>	Brindar seguimiento a los procesos de registro y compra de usuarios. Dar de alta la información de servicios y productos correspondientes al área de educación continua.

<b>Obligaciones*:</b>	Monitorear las compras realizadas y conciliar las inscripciones en el “Sistema de Gestión de Formación docente y Educación continua”
<b>(Nombre del Usuario 4*)</b>	<b>Oscar Escamilla González</b>
<b>Cargo*:</b>	Jefe de Departamento de Desarrollos Digitales para la formación Docente
<b>Funciones*:</b>	Dar mantenimiento al sistema, crear respaldo, así como brindar soporte técnico a los usuarios. Administrar la configuración del sitio, usuarios, roles, crear tiendas, publicar productos.
<b>Obligaciones*:</b>	Supervisar que el sistema esté funcionando adecuadamente y resolver las incidencias que se detecten.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente</b>	
<b>Identificador único*</b>	CUAIEED-DIEDCFD-002
<b>(Nombre del sistema A1*)</b>	Tienda Virtual CUAIEED
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos
<b>Características del lugar donde se resguardan los soportes: *</b>	

Figura 1. Diagrama de estructura

## 3. ANÁLISIS DE RIESGOS

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-002	
(Nombre del sistema A1) *	Tienda Virtual CUAIEED	
Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado a secciones administrativas del sitio.	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor.
Explotación de vulnerabilidades.	Medio	Actualización del core de CodeIgniter.
Ingreso no autorizado a cuentas de usuario compradores	Medio	Sugerir uso de contraseñas seguras a los usuarios al detectar que estas son vulnerables.
Uso de diccionarios de contraseñas para lograr el ingreso a cuentas de usuario con privilegios administrativos	Medio	Implementar el uso del servicio de reCaptcha de Google para evitar ataques automatizados. Evitar el uso de nombres de usuario obvios para usuarios con privilegios administrativos como: "admin", "root", etc.

#### 4. ANÁLISIS DE BRECHA

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-002	
(Nombre del sistema A1) *	Tienda Virtual CUAIEED	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Contraseñas seguras de usuario.	Las contraseñas de usuario con permisos administrativos deben ser únicas y rotadas constantemente para evitar el descubrimiento por medio de ataques de diccionario.	Cambio de contraseñas de usuario con privilegios administrativos cada seis meses.
Actualización de la	Tras liberarse la actualización del framework CodeIgniter 3 se deben de implementar estos	Reducir los tiempos requeridos para mantener la plataforma

plataforma	cambios inmediatamente	actualizada
------------	------------------------	-------------

## 5. PLAN DE TRABAJO

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente			
Identificador único*	CUAIEED-DIEDCFD-002		
(Nombre del sistema A1) *	Tienda Virtual CUAIEED		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización del framework	La actualización del framework permite mantener el código fuente en su última versión, con esta actividad se protege en contra de vulnerabilidades encontradas en el propio framework.	4 horas	Total
Actualización de contraseñas de usuarios	Los usuarios con privilegios administrativos deben de rotar sus contraseñas personales dentro de la plataforma para disminuir la probabilidad de un ataque por diccionario.	Continuo cada 30 días	Parcial

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único*	CUAIEED-DIEDCFD-002
(Nombre del sistema A1) *	Tienda Virtual CUAIEED

<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
<b>Transferencias mediante el traslado de soportes físicos:</b>	No se realiza tratamiento de datos personales con soportes físicos, se tiene soporte electrónico en una base de datos.
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias mediante el traslado de soportes electrónicos.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No se realizan transferencias mediante el traslado sobre redes electrónicas.

## **I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

No aplica, se tiene soporte electrónico en una base de datos.

## **II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web, almacenando la fecha, hora, dirección IP, así como las url accedidas dentro del sistema. Los archivos de log que se encuentran dentro del sistema operativo se rotan diariamente guardando una copia de las bitácoras pasadas en formato zip. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática, las herramientas utilizadas para el análisis son AWK, SED y GREP.

## **III. REGISTRO DE INCIDENTES**

Los incidentes son reportados a la Subdirección del Centro de Formación y Profesionalización para el Desarrollo Académico en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuenta con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

El tipo de soporte es electrónico por lo que la recuperación de la base de datos, la cual se encarga de almacenar los datos personales de los usuarios, es el proceso más importante. El proceso consiste en recuperar el código fuente del sistema junto con una copia de la base de datos obtenida en el proceso de respaldo programado.

Tras realizar la recuperación de los datos se realiza una comparación con un respaldo de la base de datos antes de ser comprometida para validar su estado y determinar la pertinencia de su uso.

## **V. ACCESO A LAS INSTALACIONES**

La vigilancia y el acceso físico al edificio es proporcionado por el personal de los Consejos Académicos de Área. Se cuenta con una caseta de vigilancia que registra todos los accesos para el ingreso a la Dirección de Evaluación Educativa (DEE). Para el acceso a la DEE se cuenta con un lector biométrico de huella digital, el acceso al Centro de Datos está restringido únicamente al personal autorizado de la USEE (cuenta con llave) y además tiene instalado un sistema de circuito cerrado con detección de movimiento.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

Cada usuario con rol comprador tiene la posibilidad de borrar y editar sus datos personales. En el caso donde sus datos personales son almacenados de manera colateral, como en tickets y facturas emitidas, no se puede hacer cambios o modificaciones.

## VII. PERFILES DE USUARIO Y CONTRASEÑAS

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). El sistema operativo, donde se hospedan las aplicaciones, utiliza un sistema de cuentas de usuario local que cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible. Se utiliza el algoritmo bcrypt para encriptar las contraseñas. El manejo de contraseñas es estricto para los perfiles de usuario que tienen acceso a datos personales de otras personas (Administrador, encargado de tienda y encargado administrativo). Los usuarios se pueden dar de alta ellos mismos, pero son con permisos suficientes para modificar sus propios datos personales o realizar compras y solo los usuarios con rol de administrador pueden agregar o quitar roles a los usuarios registrados.

Los usuarios trabajan con el sistema mediante una vista web, por lo que no requieren de acceso al sistema operativo donde se aloja la aplicación. Las tareas de mantenimiento de la plataforma son realizadas mediante el acceso al servidor utilizando un mecanismo de usuario y contraseña utilizando el protocolo SSH y solo se permite el acceso con cuentas de usuario limitadas. Para realizar tareas de administración en el sistema operativo es necesario ingresar las credenciales de superusuario una vez dentro del acceso remoto.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

## IX. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de negocio, el cual utiliza como fuente primordial los respaldos obtenidos de las plataformas. Las pruebas de eficiencia que se realizan han garantizado la recuperación total de la plataforma en un periodo máximo de doce horas. Actualmente no se cuenta con un sitio redundante o alternativo.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único	QUAIEED-DIEDCFD-002
Nombre del sistema A1	Tienda Virtual QUAIEED



Recurso*	Descripción*	Control*
Bitácoras del sistema	Revisión aleatoria del contenido de los logs del sistema operativo y aplicación.	Se realiza una revisión no automatizada buscando patrones de ataque conocidos y secuencias de ataques conocidos como el descubrimiento de puertos y búsqueda de archivos de configuración conocidos.  Responsables: Oscar Escamilla González

## 7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-002	
(Nombre del sistema A1) *	Tienda Virtual CUAIEED	
Medida de seguridad*	Procedimiento*	Responsable*
Revisión de permisos.	Revisiones de permisos dentro del sistema operativo, servidor web y la aplicación.	Responsable: Oscar Escamilla González. La duración es de una hora aproximadamente.
Actualización del sistema operativo.	Actualización a nuevas versiones de los paquetes del sistema operativo.	Responsable: Oscar Escamilla Gonzalez. La duración es de dos horas aproximadamente.
Actualización de la aplicación.	Actualización de Framework y bibliotecas principales del CodeIgniter 3.	Responsable: Oscar Escamilla Gonzalez. La duración es de dos horas aproximadamente.

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-002	
(Nombre del sistema A1) *	Tienda Virtual CUAIEED	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Revisión de permisos.	Se cuentan con los permisos adecuados.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.
Actualización del sistema operativo.	Se cuentan con las últimas actualizaciones.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.
Actualización de la aplicación.	Se cuentan con las últimas actualizaciones.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.

### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-002	
(Nombre del sistema A1) *	Tienda Virtual CUAIEED	
Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL.	Realizar la renovación anual del certificado SSL.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.

<i>Actualización de la aplicación.</i>	<i>Realizar el proceso de actualización de la plataforma.</i>	<i>Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.</i>
--	---	---

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

No se cuenta con un programa formal de capacitación

### 8.2. Programa de difusión de la protección a los datos personales

*(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)*

No se tiene un programa de difusión de la protección a los datos personales

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente			
Identificador único*	CUAIEED-DIEDCFD-002		
(Nombre del sistema A1) *	Tienda Virtual CUAIEED		
Actividad*	Descripción*	Duración*	Cobertura*
<i>Actualización de la plataforma a nuevas versiones.</i>	<i>Proceso de actualización con parches de seguridad del framework CodeIgniter 3.</i>	<i>1 mes.</i>	<i>Total.</i>

### 9.2. Actualización y mantenimiento de equipo de cómputo

Dirección de Desarrollo de Sistemas para la Educación			
Identificador único*	CUAIEED-DIEDCFD-002		
(Nombre del sistema A1*:	Tienda Virtual CUAIEED		
Actividad*	Descripción*	Duración*	Cobertura*
<i>Reparación o reemplazo del servidor (hardware)</i>	<i>Reparación o reemplazo del servidor en caso de fallo</i>	<i>Por evento</i>	<i>Total</i>

### 9.3. Procesos para la conservación, preservación y respaldos de información

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-002	
(Nombre del sistema A1*:	Tienda Virtual CUAIEED	
Proceso*	Descripción*	Responsable*
<i>Resguardo de unidades de almacenamiento</i>	<i>Las unidades de almacenamiento donde se realizan los respaldos automatizados se resguardan de manera indefinida</i>	<i>Unidad de Sistemas para la Evaluación Educativa (USEE)</i>

### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente
---

<b>Identificador único*</b>	CUAIEED-DIEDCFD-002	
<b>(Nombre del sistema A1*:</b>	<b>Tienda Virtual CUAIEED</b>	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
<i>Borrado seguro.</i>	<i>Formato de bajo nivel cuando se asigna el equipo.</i>  <i>Dstrucción del disco cuando es baja definitiva del equipo.</i>	<i>Unidad de Sistemas para la Evaluación Educativa (USEE).</i>

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa.

### Sistema de Registro - Jornada de Formación Docente

#### Introducción

La plataforma “Sistema de Registro - Jornada de Formación Docente”, es un sitio web donde se publica la próxima edición de la Jornada de Formación Docente que la CUAIEED organiza periódicamente. En él se publica la fecha, horario y actividades que se llevarán a cabo. Permite a los usuarios inscribirse al evento, aunque solo si son personal activo de la UNAM, ya que se hace una validación con la DGP por medio de servicios Web que él mismo ofrece. Además, ofrece funcionalidades para llevar el control de asistencia a los eventos y exportar información para el registro de los participantes en el “Sistema de Gestión de Formación Docente y Educación Continua”.

### 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente</b>	
<b>Identificador único*</b>	CUAIEED-DIEDCFD-003
<b>Nombre del sistema A1*:</b>	<b>Sistema de Registro - Jornada de Formación Docente</b>
<b>Datos personales (sensibles o no)</b>	<ul style="list-style-type: none"> <li>● Correo electrónico</li> <li>● Teléfono</li> </ul>

<b>contenidos en el sistema*:</b>	<ul style="list-style-type: none"> <li>• Datos de trabajador en la UNAM <ul style="list-style-type: none"> <li>• Nombre completo</li> <li>• Dependencias de adscripción</li> <li>• Número de trabajador</li> <li>• RFC</li> <li>• GENERO</li> </ul> </li> </ul>
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
<b>Nombre*:</b>	<b>Mtra. Ana María del Pilar Martínez Hernández</b>
<b>Cargo*:</b>	Directora de Innovación Educativa, Desarrollo Curricular y Formación Docente
<b>Funciones*:</b>	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
<b>Obligaciones*:</b>	<ul style="list-style-type: none"> <li>- Definir junto con los responsables del sistema, los tipos de acceso.</li> <li>- Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.</li> </ul>
<b>Encargados</b>	
<b>(Nombre del Encargado 1*:</b>	<b>Dra. Ruth Torres Carrasco</b>
<b>Cargo*:</b>	Subdirectora Centro de Formación y Profesionalización para el Desarrollo Académico
<b>Funciones*:</b>	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
<b>Obligaciones*:</b>	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>(Nombre del Encargado 2*:</b>	<b>Mtro. Oscar Escamilla González</b>
<b>Cargo*:</b>	Jefe de Departamento de Desarrollos Digitales para la formación Docente

<b>Funciones*:</b>	Desarrollar y dar mantenimiento al sistema, crear respaldo, así como brindar soporte técnico a los usuarios. Administrar la configuración del sitio, crear tiendas, publicar productos.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 3*:</b>	<b>Paulina Manjarrez Molina</b>
<b>Cargo*:</b>	Jefa del Departamento de Educación Continua y Extensión Académica
<b>Funciones*:</b>	Brindar seguimiento a los procesos de registro y compra de usuarios.
<b>Obligaciones*:</b>	Cumplir con la obligación legal de resguardar los datos personales.
<b>(Nombre del Encargado 4*:</b>	<b>Mtra. Dulce Campos del Razo</b>
<b>Cargo*:</b>	Subdirectora de Informática y Proyectos de Tecnologías de la Información
<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>Usuarios:</b>	
<b>(Nombre del Usuario *)</b>	Docentes y personal de la UNAM.
<b>Cargo*:</b>	Comunidad académica y funcionarios de la UNAM
<b>Funciones*:</b>	Consultar la información de próximos eventos, inscribirse a las actividades de su preferencia.

<b>Obligaciones*:</b>	Validar su inscripción y asistir a los eventos.
<b>(Nombre del Usuario 2*)</b>	<b>Paulina Manjarrez Molina</b>
<b>Cargo*:</b>	Jefa del Departamento de Educación Continua y Extensión Académica
<b>Funciones*:</b>	Brindar seguimiento a los procesos de registro y cupo en las actividades.
<b>Obligaciones*:</b>	Monitorear los registros de personas a las distintas actividades, generar listas de asistencia y consolidar los reportes de asistencia dentro del sistema.
<b>(Nombre del Usuario 4*)</b>	<b>Oscar Escamilla González</b>
<b>Cargo*:</b>	Jefe de Departamento de Desarrollos Digitales para la formación Docente
<b>Funciones*:</b>	Dar mantenimiento al sistema, crear respaldo, así como brindar soporte técnico a los usuarios. Administrar la configuración del sitio, usuarios, roles, cargar información de los eventos y actividades.
<b>Obligaciones*:</b>	Supervisar que el sistema esté funcionando adecuadamente y resolver las incidencias que se detecten.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente</b>	
<b>Identificador único*</b>	CUAIEED-DIEDCFD-003
<b>(Nombre del sistema A1*)</b>	Sistema de Registro - Jornada de Formación Docente
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos
<b>Características del lugar donde se resguardan los soportes: *</b>	Alojamiento en el centro de datos de la CUAIEED dentro de diversas máquinas virtuales, el cual cuenta con acceso mediante un sistema biométrico, planta de energía eléctrica, sistema de respaldo de energía eléctrica ininterrumpida (UPS) y aire acondicionado seco.

## 3. ANÁLISIS DE RIESGOS



Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-003	
(Nombre del sistema A1) *	Sistema de Registro - Jornada de Formación Docente	
Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado a secciones administrativas del sitio.	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor.
Explotación de vulnerabilidades.	Medio	Actualización del core de CodeIgniter 4.
Ingreso no autorizado a cuentas de usuario compradores	Medio	Sugerir uso de contraseñas seguras a los usuarios al detectar que estas son vulnerables.
Uso de diccionarios de contraseñas para lograr el ingreso a cuentas de usuario con privilegios administrativos	Medio	Implementar el uso del servicio de reCaptcha de Google para evitar ataques automatizados. Evitar el uso de nombres de usuario obvios para usuarios con privilegios administrativos como: "admin", "root", etc.

#### 4. ANÁLISIS DE BRECHA

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-003	
(Nombre del sistema A1) *	Sistema de Registro - Jornada de Formación Docente	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Contraseñas seguras de usuario.	Las contraseñas de usuario con permisos administrativos deben ser únicas y rotadas constantemente para evitar el descubrimiento por medio de ataques de diccionario.	Cambio de contraseñas de usuario con privilegios administrativos cada seis meses.

Actualización de la plataforma.	Tras liberarse la actualización del framework CodeIgniter 4 se deben de implementar estos cambios inmediatamente.	Reducir los tiempos requeridos para mantener la plataforma actualizada.
---------------------------------	---	---

## 5. PLAN DE TRABAJO

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente			
Identificador único*	CUAIEED-DIEDCFD-003		
(Nombre del sistema A1) *	Sistema de Registro - Jornada de Formación Docente		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización del framework	La actualización del framework permite mantener el código fuente en su última versión, con esta actividad se protege en contra de vulnerabilidades encontradas en el propio framework.	4 horas	Total
Actualización de contraseñas de usuarios.	Los usuarios con privilegios administrativos deben de rotar sus contraseñas personales dentro de la plataforma para disminuir la probabilidad de un ataque por diccionario.	Continuo cada 30 días	Parcial

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único*	CUAIEED-DIEDCFD-003

<b>(Nombre del sistema A1) *</b>	<b>Sistema de Registro - Jornada de Formación Docente</b>
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
<b>Transferencias mediante el traslado de soportes físicos:</b>	No se realiza tratamiento de datos personales con soportes físicos, se tiene soporte electrónico en una base de datos.
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias mediante el traslado de soportes electrónicos.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	Se exporta un archivo en formato "csv" para integrarse al "Sistema de Gestión de Formación Docente y Educación Continua". Este se transporta por medio de correo electrónico en formato zip protegido con contraseña.

### **I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

No aplica, se tiene soporte electrónico en una base de datos.

### **II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web, almacenando la fecha, hora, dirección IP, así como las url accedidas dentro del sistema. Los archivos de log que se encuentran dentro del sistema operativo se rotan diariamente guardando una copia de las bitácoras pasadas en formato zip. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática, las herramientas utilizadas para el análisis son AWK, SED y GREP.

### **III. REGISTRO DE INCIDENTES**

Los incidentes son reportados a la Subdirección del Centro de Formación y Profesionalización para el Desarrollo Académico en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuenta con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses. El tipo de soporte es electrónico por lo que la recuperación de la base de datos, la cual se encarga de almacenar los datos personales de los usuarios, es el proceso más importante. El proceso consiste en recuperar el código fuente del sistema junto con una copia de la base de datos obtenida en el proceso de respaldo programado.

Tras realizar la recuperación de los datos se realiza una comparación con un respaldo de la base de datos antes de ser comprometida para validar su estado y determinar la pertinencia de su uso.

### **V. ACCESO A LAS INSTALACIONES**

CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente. La dependencia se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por la directora de Innovación Educativa, Desarrollo Curricular y Formación Docente.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

No hay procedimiento de corrección de datos personales ya que estos no se obtienen directamente del usuario, sino que son recuperados desde la base de datos de la dirección general de personal de la UNAM.

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). El sistema operativo, donde se hospedan las aplicaciones, utiliza un sistema de cuentas de usuario local que cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible. Se utiliza el algoritmo bcrypt para encriptar las contraseñas. El manejo de contraseñas es estricto para los perfiles de usuario que tienen acceso a datos personales de otras personas (Administrador, supervisor de actividades).

Los usuarios trabajan con el sistema mediante una vista web, por lo que no requieren de acceso al sistema operativo donde se aloja la aplicación. Las tareas de mantenimiento de la plataforma son realizadas mediante el acceso al servidor utilizando un mecanismo de llave pública/privada, solamente los administradores de la plataforma pueden realizar este proceso. La protección contra los accesos no autorizados se realiza mediante el filtrado de puertos y el sistema antes mencionado de llaves públicas y privadas en donde el servidor no acepta accesos mediante contraseña.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

Las plataformas son respaldadas utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello, por un promedio de treinta días tras, y almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas seguras y en condiciones óptimas para su funcionamiento. Para promover la conservación y preservación de la información, las cintas y el lector de estas se mantienen por tiempo indefinido.

## **IX. PLAN DE CONTINGENCIA**

Se cuenta con un plan de contingencia que permite la continuidad de negocio, el cual utiliza como fuente primordial los respaldos obtenidos de las plataformas en cintas magnéticas y en un servidor dedicado. Las pruebas de eficiencia que se realizan han garantizado la recuperación total de la plataforma en un periodo máximo de doce horas. Actualmente no se cuenta con un sitio redundante

o alterno.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-003	
(Nombre del sistema A1) *	Sistema de Registro - Jornada de Formación Docente	
Recurso*	Descripción*	Control*
Bitácoras del sistema	Revisión aleatoria del contenido de los logs del sistema operativo y aplicación.	Se realiza una revisión no automatizada buscando patrones de ataque conocidos y secuencias de ataques conocidas como el descubrimiento de puertos y búsqueda de archivos de configuración conocidos.  Responsables: Oscar Escamilla González

### 7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-003	
(Nombre del sistema A1) *	Sistema de Registro - Jornada de Formación Docente	
Medida de seguridad*	Procedimiento*	Responsable*

Revisión de permisos.	Revisión de permisos dentro del sistema operativo, servidor web y la aplicación.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.
Actualización del sistema operativo.	Actualización a nuevas versiones de los paquetes del sistema operativo.	Responsable: Oscar Escamilla Gonzalez. La duración es de dos horas aproximadamente.
Actualización de la aplicación.	Actualización de Framework y bibliotecas principales del CodeIgniter 4.	Responsable: Oscar Escamilla Gonzalez. La duración es de dos horas aproximadamente.

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-003	
(Nombre del sistema A1) *	Sistema de Registro - Jornada de Formación Docente	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Revisión de permisos.	Se cuentan con los permisos adecuados.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.
Actualización del sistema operativo.	Se cuentan con las últimas actualizaciones.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.
Actualización de la aplicación.	Se cuentan con las últimas actualizaciones.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.

### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente
---

Identificador único*	CUAIEED-DIEDCFD-003	
(Nombre del sistema A1) *	Sistema de Registro - Jornada de Formación Docente	
Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL.	Realizar la renovación anual del certificado SSL.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.
Actualización de la aplicación.	Realizar el proceso de actualización de la plataforma.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

No se cuenta con un programa formal de capacitación

### 8.2. Programa de difusión de la protección a los datos personales

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

No se tiene un programa de difusión de la protección a los datos personales

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único*	CUAIEED-DIEDCFD-003

<b>(Nombre del sistema A1) *</b>		<b>Sistema de Registro - Jornada de Formación Docente</b>	
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
<i>Actualización de la plataforma a nuevas versiones.</i>	<i>Proceso de actualización con parches de seguridad de CodeIgniter 4.</i>	<i>1 mes.</i>	<i>Total.</i>

### 9.2. Actualización y mantenimiento de equipo de cómputo

<b>Dirección de Desarrollo de Sistemas para la Educación</b>			
<b>Identificador único*</b>	CUAIEED-DIEDCFD-003		
<b>(Nombre del sistema A1*:</b>	<b>Sistema de Registro - Jornada de Formación Docente</b>		
<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
<i>Reparación o reemplazo del servidor (hardware)</i>	<i>Reparación o reemplazo del servidor en caso de fallo</i>	<i>Por evento</i>	<i>Total</i>

### 9.3. Procesos para la conservación, preservación y respaldos de información

<b>Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente</b>	
<b>Identificador único*</b>	CUAIEED-DIEDCFD-003
<b>(Nombre del sistema A1*:</b>	<b>Sistema de Registro - Jornada de Formación Docente</b>



Proceso*	Descripción*	Responsable*
<i>Resguardo de cintas magnéticas.</i>	<i>Las cintas magnéticas realizadas en la fase de respaldo automatizado y el lector de las cintas magnéticas son resguardadas de forma indefinida.</i>	<i>Departamento de Operaciones y Seguridad Informática.</i>

#### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
<b>Identificador único*</b>	CUAIEED-DIEDCFD-003	
<b>(Nombre del sistema A1*:</b>	<b>Sistema de Registro - Jornada de Formación Docente</b>	
Proceso*	Descripción*	Responsable*
<i>Borrado seguro.</i>	<i>Se realiza un formato de bajo nivel al disco duro físico del hipervisor.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.</i>

### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El director de la Dirección de Desarrollo de Sistemas para la Educación recibe o envía la petición en donde se indica la razón para la cancelación del sistema, el tiempo que deberá de permanecer la plataforma funcionando antes de ser eliminada y si se necesita entregar un respaldo final del sistema para su resguardo final en un soporte electrónico. La petición siempre es en formato escrito ya sea por correo electrónico o por oficio. El sistema será eliminado tras una fecha de término establecida y se borra de forma permanente la máquina virtual donde este reside.

#### Catálogo de Insumos Audiovisuales Didácticos Digitales

##### Introducción

La plataforma “Catálogo de Insumos Audiovisuales Didácticos Digitales”, es un sitio web donde se tiene publicado un catálogo de ilustraciones y fotografías cuyo propósito es ofrecer a la comunidad

universitaria y al público en general estos como insumos para desarrollar materiales didácticos bajo una licencia Creative Commons [Atribución-No comercial-Compartir igual](#). Se solicita a los usuarios registrarse para poder descargar los recursos, así como el proyecto/material en donde utilizarán cada recurso para tener un registro/evidencia de donde se están utilizando estos materiales.

## 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente</b>	
<b>Identificador único*</b>	CUAIEED-DIEDCFD-004
<b>Nombre del sistema A1*:</b>	<b><u>Catálogo de Insumos Audiovisuales Didácticos Digitales</u></b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Correo electrónico, Nombre completo, Nombre, url (opcional)
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
<b>Nombre*:</b>	<b>Mtra. Ana María del Pilar Martínez Hernández</b>
<b>Cargo*:</b>	Directora de Innovación Educativa, Desarrollo Curricular y Formación Docente
<b>Funciones*:</b>	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
<b>Obligaciones*:</b>	<ul style="list-style-type: none"> <li>- Definir junto con los responsables del sistema, los tipos de acceso.</li> <li>- Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.</li> </ul>
<b>Encargados</b>	
<b>(Nombre del Encargado 1) *:</b>	<b>Dra. Ruth Torres Carrasco</b>
<b>Cargo*:</b>	Subdirectora Centro de Formación y Profesionalización para el Desarrollo Académico

<b>Funciones*:</b>	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
<b>Obligaciones*:</b>	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>(Nombre del Encargado 2*):</b>	<b>Mtro. Oscar Escamilla González</b>
<b>Cargo*:</b>	Jefe de Departamento de Desarrollos Digitales para la formación Docente
<b>Funciones*:</b>	Desarrollar y dar mantenimiento al sistema, crear respaldo, así como brindar soporte técnico a los usuarios. Administrar la configuración del sitio, crear tiendas, publicar productos.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 3*):</b>	<b>Ing. Carlos Alberto Jaimes Vergara</b>
<b>Cargo*:</b>	Coordinador Formación Digital y Recursos Audiovisuales para la Docencia
<b>Funciones*:</b>	Desarrollar y dar mantenimiento al sistema, crear respaldo, así como brindar soporte técnico a los usuarios. Administrar la configuración del sitio, crear tiendas, publicar productos.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 4*):</b>	<b>Mtra. Dulce Campos del Razo</b>
<b>Cargo*:</b>	Subdirectora de Informática y Proyectos de Tecnologías de la Información
<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.

<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>Usuarios:</b>	
<b>(Nombre del Usuario *)</b>	Público en general, en particular Docentes y personal de la UNAM.
<b>Cargo*:</b>	Comunidad académica.
<b>Funciones*:</b>	Buscar en el catálogo y descargar insumos digitales
<b>Obligaciones*:</b>	Informar sobre los usos que se les dé a las imágenes descargadas y respetar los acuerdos de licencia de uso publicados en el sitio.
<b>(Nombre del Usuario 2*)</b>	<b>Oscar Escamilla González</b>
<b>Cargo*:</b>	Jefe de Departamento de Desarrollos Digitales para la formación Docente
<b>Funciones*:</b>	Dar mantenimiento al sistema, crear respaldo, así como brindar soporte técnico a los usuarios. Administrar la configuración del sitio, usuarios, roles, cargar información de los eventos y actividades. Gestionar la publicación de los recursos multimedia
<b>Obligaciones*:</b>	Supervisar que el sistema esté funcionando adecuadamente y resolver las incidencias que se detecten.
<b>(Nombre del Usuario 2*)</b>	<b>Carlos Alberto Jaimes Vergara</b>
<b>Cargo*:</b>	Coordinador Formación Digital y Recursos Audiovisuales para la Docencia
<b>Funciones*:</b>	Dar mantenimiento al sistema, crear respaldo, así como brindar soporte técnico a los usuarios. Administrar la configuración del sitio, usuarios, roles, cargar información de los eventos y actividades. Gestionar la publicación de los recursos multimedia

<b>Obligaciones*:</b>	Supervisar que el sistema esté funcionando adecuadamente y resolver las incidencias que se detecten.
-----------------------	--

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente	
<b>Identificador único*</b>	CUAIEED-DIEDCFD-004
<b>(Nombre del sistema A1*)</b>	Catálogo de Insumos Audiovisuales Didácticos Digitales
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos
<b>Características del lugar donde se resguardan los soportes: *</b>	Alojamiento en el centro de datos de CUAIEED dentro de diversas máquinas virtuales, el cual cuenta con acceso mediante un sistema biométrico, planta de energía eléctrica, sistema de respaldo de energía eléctrica ininterrumpida (UPS) y aire acondicionado seco.

## 3. ANÁLISIS DE RIESGOS

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
<b>Identificador único*</b>	CUAIEED-DIEDCFD-004	
<b>(Nombre del sistema A1) *</b>	Catálogo de Insumos Audiovisuales Didácticos Digitales	
<b>Riesgo*</b>	<b>Impacto*</b>	<b>Mitigación*</b>
Ingreso no autorizado a secciones administrativas del sitio.	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor.
Explotación de vulnerabilidades.	Medio	Actualización del core de CodeIgniter 4.
Ingreso no autorizado a cuentas de usuario compradores.	Medio	Sugerir uso de contraseñas seguras a los usuarios al detectar que estas son vulnerables.

Uso de diccionarios de contraseñas para lograr el ingreso a cuentas de usuario con privilegios administrativos	Medio	Implementar dentro de la página de ingreso, el uso del servicio de reCaptcha de Google para evitar ataques automatizados. Evitar el uso de nombres de usuario obvios para usuarios con privilegios administrativos como: "admin", "root", etc.
--	-------	--

#### 4. ANÁLISIS DE BRECHA

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-004	
(Nombre del sistema A1) *	Catálogo de Insumos Audiovisuales Didácticos Digitales	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Contraseñas seguras de usuario.	Las contraseñas de usuario con permisos administrativos deben ser únicas y rotadas constantemente para evitar el descubrimiento por medio de ataques de diccionario.	Cambio de contraseñas de usuario con privilegios administrativos cada seis meses.
Actualización de la plataforma	Tras liberarse la actualización del framework CodeIgniter 4 se deben de implementar estos cambios inmediatamente.	Reducir los tiempos requeridos para mantener la plataforma actualizada.

#### 5. PLAN DE TRABAJO

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único*	CUAIEED-DIEDCFD-004
(Nombre del sistema A1) *	Catálogo de Insumos Audiovisuales Didácticos Digitales

Actividad*	Descripción*	Duración*	Cobertura*
Actualización del framework	La actualización del framework permite mantener el código fuente en su última versión, con esta actividad se protege en contra de vulnerabilidades encontradas en el propio framework.	4 horas	Total
Actualización de contraseñas de usuarios.	Los usuarios con privilegios administrativos deben de rotar sus contraseñas personales dentro de la plataforma para disminuir la probabilidad de un ataque por diccionario.	Continuo cada 30 días	Parcial

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único*	CUAIEED-DIEDCFD-004
(Nombre del sistema A1) *	<b>Catálogo de Insumos Audiovisuales Didácticos Digitales</b>
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
<b>Transferencias mediante el traslado de soportes físicos:</b>	No se realiza tratamiento de datos personales con soportes físicos, se tiene soporte electrónico en una base de datos.
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias mediante el traslado de soportes electrónicos.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	Se exporta un archivo en formato "csv" para integrarse al "Sistema de Gestión de Formación Docente y Educación Continua". Este se transporta por medio de correo electrónico en formato zip protegido con contraseña.

## **I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

No aplica, se tiene soporte electrónico en una base de datos.

## **II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web, almacenando la fecha, hora, dirección IP, así como las url accedidas dentro del sistema. Los archivos de log que se encuentran dentro del sistema operativo se rotan diariamente guardando una copia de las bitácoras pasadas en formato zip. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática, las herramientas utilizadas para el análisis son AWK, SED y GREP.

## **III. REGISTRO DE INCIDENTES**

Los incidentes son reportados a la Subdirección del Centro de Formación y Profesionalización para el Desarrollo Académico en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuenta con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

El tipo de soporte es electrónico por lo que la recuperación de la base de datos, la cual se encarga de almacenar los datos personales de los usuarios, es el proceso más importante. El proceso consiste en recuperar el código fuente del sistema junto con una copia de la base de datos obtenida en el proceso de respaldo programado.

Tras realizar la recuperación de los datos se realiza una comparación con un respaldo de la base de datos antes de ser comprometida para validar su estado y determinar la pertinencia de su uso.

## **V. ACCESO A LAS INSTALACIONES**

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente. La dependencia se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por la directora de Innovación Educativa, Desarrollo Curricular y Formación Docente.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

Cada usuario tiene acceso a modificar o eliminar sus datos personales registrados en el sistema.

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**



El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). El sistema operativo, donde se hospedan las aplicaciones, utiliza un sistema de cuentas de usuario local que cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible. Se utiliza el algoritmo bcrypt para encriptar las contraseñas. El manejo de contraseñas es estricto para los perfiles de usuario, aunque hay una parte pública desde la cual no se tiene acceso a ningún dato personal.

Los usuarios trabajan con el sistema mediante una vista web, por lo que no requieren de acceso al sistema operativo donde se aloja la aplicación. Las tareas de mantenimiento de la plataforma son realizadas mediante el acceso al servidor utilizando un mecanismo de llave pública/privada, solamente los administradores de la plataforma pueden realizar este proceso. La protección contra los accesos no autorizados se realiza mediante el filtrado de puertos y el sistema antes mencionado de llaves públicas y privadas en donde el servidor no acepta accesos mediante contraseña.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Las plataformas son respaldadas utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello, por un promedio de treinta días tras, y almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas seguras y en condiciones óptimas para su funcionamiento. Para promover la conservación y preservación de la información, las cintas y el lector de estas se mantienen por tiempo indefinido.

## IX. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de negocio, el cual utiliza como fuente primordial los respaldos obtenidos de las plataformas en cintas magnéticas y en un servidor dedicado. Las pruebas de eficiencia que se realizan han garantizado la recuperación total de la plataforma en un periodo máximo de doce horas. Actualmente no se cuenta con un sitio redundante o alterno.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único:	GJAI EED-DIEDCFD-004	
(Nombre del sistema A1):	Catálogo de Insumos Audiovisuales Didácticos Digitales	
Recurso	Descripción	Control

<p>Bitácoras del sistema</p>	<p>Revisión aleatoria del contenido de los logs del sistema operativo y aplicación.</p>	<p>Se realiza una revisión no automatizada buscando patrones de ataque conocidos y secuencias de ataques conocidas como el descubrimiento de puertos y búsqueda de archivos de configuración conocidos.</p> <p>Responsables: Oscar Escamilla González</p>
------------------------------	---	---

### 7.2. Procedimiento para la revisión de las medidas de seguridad

<p>Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente</p>		
<p>Identificador único*</p>	<p>CUAIEED-DIEDCFD-004</p>	
<p>(Nombre del sistema A1) *</p>	<p>Catálogo de Insumos Audiovisuales Didácticos Digitales</p>	
<p>Medida de seguridad*</p>	<p>Procedimiento*</p>	<p>Responsable*</p>
<p>Revisión de permisos.</p>	<p>Revisión de permisos dentro del sistema operativo, servidor web y la aplicación.</p>	<p>Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.</p>
<p>Actualización del sistema operativo.</p>	<p>Actualización a nuevas versiones de los paquetes del sistema operativo.</p>	<p>Responsable: Oscar Escamilla Gonzalez. La duración es de dos horas aproximadamente.</p>
<p>Actualización de la aplicación.</p>	<p>Actualización de Framework y bibliotecas principales del CodeIgniter 4.</p>	<p>Responsable: Oscar Escamilla Gonzalez. La duración es de dos horas aproximadamente.</p>

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

<p>Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente</p>
--

Identificador único*	CUAIEED-DIEDCFD-004	
(Nombre del sistema A1) *	Catálogo de Insumos Audiovisuales Didácticos Digitales	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Revisión de permisos.	Se cuentan con los permisos adecuados.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.
Actualización del sistema operativo.	Se cuentan con las últimas actualizaciones.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.
Actualización de la aplicación.	Se cuentan con las últimas actualizaciones.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.

#### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-004	
(Nombre del sistema A1) *	Catálogo de Insumos Audiovisuales Didácticos Digitales	
Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL.	Realizar la renovación anual del certificado SSL.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.
Actualización de la aplicación.	Realizar el proceso de actualización de la plataforma.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

**8.1. Programa de capacitación a los responsables de seguridad de datos personales**

No se cuenta con un programa formal de capacitación

**8.2. Programa de difusión de la protección a los datos personales**

*(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)*

No se tiene un programa de difusión de la protección a los datos personales

**9. MEJORA CONTINUA**

**9.1. Actualización y mantenimiento de sistemas de información**

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente			
Actividad*	Descripción*	Duración*	Cobertura*
Identificador único*	CUAIEED-DIEDCFD-004		
(Nombre del sistema A1) *	Catálogo de Insumos Audiovisuales Didácticos Digitales		
<i>Actualización de la plataforma a nuevas versiones.</i>	<i>Proceso de actualización con parches de seguridad de CodeIgniter 4.</i>	<i>1 mes.</i>	<i>Total.</i>

**9.2. Actualización y mantenimiento de equipo de cómputo**

Dirección de Desarrollo de Sistemas para la Educación	
Identificador único*	CUAIEED-DIEDCFD-004
(Nombre del sistema A1*:	Catálogo de Insumos Audiovisuales Didácticos Digitales

Actividad*	Descripción*	Duración*	Cobertura*
<i>Reparación o reemplazo del servidor (hardware)</i>	<i>Reparación o reemplazo del servidor en caso de fallo</i>	<i>Por evento</i>	<i>Total</i>

### 9.3. Procesos para la conservación, preservación y respaldos de información

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
<b>Identificador único*</b>	CUAIEED-DIEDCFD-004	
<b>(Nombre del sistema A1*:</b>	<b>Catálogo de Insumos Audiovisuales Didácticos Digitales</b>	
Proceso*	Descripción*	Responsable*
<i>Resguardo de cintas magnéticas.</i>	<i>Las cintas magnéticas realizadas en la fase de respaldo automatizado y el lector de las cintas magnéticas son resguardadas de forma indefinida.</i>	<i>Departamento de Operaciones y Seguridad Informática.</i>

### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
<b>Identificador único*</b>	CUAIEED-DIEDCFD-004	
<b>(Nombre del sistema A1*:</b>	<b>Catálogo de Insumos Audiovisuales Didácticos Digitales</b>	
Proceso*	Descripción*	Responsable*

<i>Borrado seguro.</i>	<i>Se realiza un formato de bajo nivel al disco duro físico del hipervisor.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.</i>
------------------------	---	---

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El director de la Dirección de Desarrollo de Sistemas para la Educación recibe o envía la petición en donde se indica la razón para la cancelación del sistema, el tiempo que deberá de permanecer la plataforma funcionando antes de ser eliminada y si se necesita entregar un respaldo final del sistema para su resguardo final en un soporte electrónico. La petición siempre es en formato escrito ya sea por correo electrónico o por oficio. El sistema será eliminado tras una fecha de término establecida y se borra de forma permanente la máquina virtual donde este reside.

### Resultados de Evaluación de Actividades de Formación Docente

#### Introducción

La plataforma “Resultados de Evaluación de Actividades de Formación Docente”, es un sitio web donde se tienen publicados los resultados obtenidos por cada una de las actividades de formación docentes impartidas en la coordinación, así como datos estadísticos sobre la inscripción a estas. En el sitio se despliega una lista de todas las actividades, así como la evaluación individual de cada una junto con datos estadísticos sobre la inscripción y calificaciones de los participantes. Opcionalmente se puede descargar un archivo en formato pdf por cada actividad. Cabe destacar que el despliegue de los reportes solo cuenta con datos estadísticos de las inscripciones y el único dato personal que se muestra en estos es el nombre completo de los integrantes del cuerpo docente que imparte la actividad.

La información de las actividades, como las personas inscritas y el cuerpo docente se toman del “Sistema de Gestión de Formación Docente y Educación Continua” de la CUAIEED y la evaluación es generada a partir de un formulario donde los asistentes plasman su satisfacción con respectos a varios aspectos de las actividades. Este sistema es de uso interno y el acceso está restringido a personal de la Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente.

### 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente</b>	
<b>Identificador único*</b>	<b>CUAIEED-DIEDCFD-005</b>
<b>Nombre del sistema A1*:</b>	<b>Resultados de Evaluación de Actividades de Formación Docente</b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Correo electrónico, Nombre completo, Dependencias de adscripción, Número de trabajador, RFC, Genero

<b>Responsable*:</b>	<b>Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).</b>
<b>Nombre*:</b>	Mtra. Ana María del Pilar Martínez Hernández
<b>Cargo*:</b>	Directora de Innovación Educativa, Desarrollo Curricular y Formación Docente
<b>Funciones*:</b>	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
<b>Obligaciones*:</b>	<ul style="list-style-type: none"> <li>- Definir junto con los responsables del sistema, los tipos de acceso.</li> <li>- Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.</li> </ul>
<b>Encargados</b>	
<b>(Nombre del Encargado 1*:</b>	Dra. Ruth Torres Carrasco
<b>Cargo*:</b>	Subdirectora Centro de Formación y Profesionalización para el Desarrollo Académico
<b>Funciones*:</b>	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
<b>Obligaciones*:</b>	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>(Nombre del Encargado 2*):</b>	Mtro. Oscar Escamilla González
<b>Cargo*:</b>	Jefe de Departamento de Desarrollos Digitales para la formación Docente
<b>Funciones*:</b>	Desarrollar y dar mantenimiento al sistema, crear respaldo, así como brindar soporte técnico a los usuarios. Administrar la configuración del sitio, crear tiendas, publicar productos.

<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>(Nombre del Encargado 3) *:</b>	Paulina Manjarrez Molina
<b>Cargo*:</b>	Jefa del Departamento de Educación Continua y Extensión Académica
<b>Funciones*:</b>	Revisar y descargar las evaluaciones de cada actividad.
<b>Obligaciones*:</b>	Cumplir con la obligación legal de resguardar los datos personales.
<b>(Nombre del Encargado 4) *:</b>	Mtra. Dulce Campos del Razo
<b>Cargo*:</b>	Subdirectora de Informática y Proyectos de Tecnologías de la Información
<b>Funciones*:</b>	Asegurar el funcionamiento de la infraestructura física y virtual de los sistemas o servidores de la Coordinación.
<b>Obligaciones*:</b>	Realizar la protección a nivel hardware y software de los servidores físicos y virtuales, de las bases de datos, así como los procesos de actualización de la plataforma.
<b>Usuarios:</b>	
<b>(Nombre del Usuario 1*)</b>	Oscar Escamilla González
<b>Cargo*:</b>	Jefe de Departamento de Desarrollos Digitales para la formación Docente
<b>Funciones*:</b>	Dar mantenimiento al sistema, crear respaldo, así como brindar soporte técnico a los usuarios. Administrar la configuración del sitio, usuarios, roles, cargar información de los eventos y actividades.
<b>Obligaciones*:</b>	Supervisar que el sistema esté funcionando adecuadamente y resolver las incidencias que se detecten.



<b>(Nombre del Usuario 2*)</b>	Paulina Manjarrez Molina
<b>Cargo*:</b>	Jefa del Departamento de Educación Continua y Extensión Académica
<b>Funciones*:</b>	Revisar y descargar las evaluaciones de cada actividad.
<b>Obligaciones*:</b>	Revisar que la información esté actualizada, compartir la evaluación de cada actividad con el responsable académico de esta. Reportar errores o inconsistencias.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente	
<b>Identificador único*</b>	CUAIEED-DIEDCFD-005
<b>(Nombre del sistema A1*)</b>	Resultados de Evaluación de Actividades de Formación Docente
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Base de datos
<b>Características del lugar donde se resguardan los soportes: *</b>	Alojamiento en el centro de datos de CUAIEED dentro de diversas máquinas virtuales, el cual cuenta con acceso mediante un sistema biométrico, planta de energía eléctrica, sistema de respaldo de energía eléctrica ininterrumpida (UPS) y aire acondicionado seco.

## 3. ANÁLISIS DE RIESGOS

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
<b>Identificador único*</b>	CUAIEED-DIEDCFD-005	
<b>(Nombre del sistema A1) *</b>	Resultados de Evaluación de Actividades de Formación Docente	
<b>Riesgo*</b>	<b>Impacto*</b>	<b>Mitigación*</b>

Ingreso no autorizado a secciones administrativas del sitio.	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor.
Explotación de vulnerabilidades.	Medio	Actualización del core de CodeIgniter 4.
Ingreso no autorizado a cuentas de usuario compradores	Medio	Sugerir uso de contraseñas seguras a los usuarios al detectar que estas son vulnerables.
Uso de diccionarios de contraseñas para lograr el ingreso a cuentas de usuario con privilegios administrativos	Medio	Implementar dentro de la página de ingreso, el uso del servicio de reCaptcha de Google para evitar ataques automatizados. Evitar el uso de nombres de usuario obvios para usuarios con privilegios administrativos como: "admin", "root", etc.

#### 4. ANÁLISIS DE BRECHA

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-005	
(Nombre del sistema A1) *	Resultados de Evaluación de Actividades de Formación Docente	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Contraseñas seguras de usuario.	Las contraseñas de usuario con permisos administrativos deben ser únicas y rotadas constantemente para evitar el descubrimiento por medio de ataques de diccionario.	Cambio de contraseñas de usuario con privilegios administrativos cada seis meses.
Actualización de la plataforma.	Tras liberarse la actualización del framework CodeIgniter 4 se deben de implementar estos cambios inmediatamente.	Reducir los tiempos requeridos para mantener la plataforma actualizada.

## 5. PLAN DE TRABAJO

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente			
Identificador único*	CUAIEED-DIEDCFD-005		
(Nombre del sistema A1) *	Resultados de Evaluación de Actividades de Formación Docente		
Actividad*	Descripción*	Duración*	Cobertura*
Actualización del framework	La actualización del framework permite mantener el código fuente en su última versión, con esta actividad se protege en contra de vulnerabilidades encontradas en el propio framework.	4 horas	Total
Actualización de contraseñas de usuarios.	Los usuarios con privilegios administrativos deben de rotar sus contraseñas personales dentro de la plataforma para disminuir la probabilidad de un ataque por diccionario.	Continuo cada 30 días	Parcial

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único*	CUAIEED-DIEDCFD-005
(Nombre del sistema A1) *	Resultados de Evaluación de Actividades de Formación Docente
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	

<b>Transferencias mediante el traslado de soportes físicos:</b>	No se realiza tratamiento de datos personales con soportes físicos, se tiene soporte electrónico en una base de datos.
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias mediante el traslado de soportes electrónicos.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No se realizan transferencias mediante el traslado sobre redes electrónicas.

## **I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

**No aplica, se tiene soporte electrónico en una base de datos.**

## **II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web, almacenando la fecha, hora, dirección IP, así como las url accedidas dentro del sistema. Los archivos de log que se encuentran dentro del sistema operativo se rotan diariamente guardando una copia de las bitácoras pasadas en formato zip. Las bitácoras son analizadas por el Departamento de Operaciones y Seguridad Informática, las herramientas utilizadas para el análisis son AWK, SED y GREP.

## **III. REGISTRO DE INCIDENTES**

Los incidentes son reportados a la Subdirección del Centro de Formación y Profesionalización para el Desarrollo Académico en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la gravedad de la incidencia. Se cuenta con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

El tipo de soporte es electrónico por lo que la recuperación de la base de datos, la cual se encarga de almacenar los datos personales de los usuarios, es el proceso más importante. El proceso consiste en recuperar el código fuente del sistema junto con una copia de la base de datos obtenida en el proceso de respaldo programado.

Tras realizar la recuperación de los datos se realiza una comparación con un respaldo de la base de datos antes de ser comprometida para validar su estado y determinar la pertinencia de su uso.

## **V. ACCESO A LAS INSTALACIONES**

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente. La dependencia se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de

biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por la directora de Innovación Educativa, Desarrollo Curricular y Formación Docente.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

No hay procedimiento de corrección de datos personales ya que estos se obtienen directamente del “Sistema de Gestión de Formación Docente y Educación Continua” y al ser de uso interno, los datos personales almacenados no están a la vista de los individuos susceptibles a solicitar cambios en sus datos personales.

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). El sistema operativo, donde se hospedan las aplicaciones, utiliza un sistema de cuentas de usuario local que cifra las contraseñas de los usuarios utilizando una función de Hash la cual no es reversible. Se utiliza el algoritmo bcrypt para encriptar las contraseñas. El manejo de contraseñas es estricto para los perfiles de usuario, aunque hay una parte pública desde la cual no se tiene acceso a ningún dato personal.

Los usuarios trabajan con el sistema mediante una vista web, por lo que no requieren de acceso al sistema operativo donde se aloja la aplicación. Las tareas de mantenimiento de la plataforma son realizadas mediante el acceso al servidor utilizando un mecanismo de llave pública/privada, solamente los administradores de la plataforma pueden realizar este proceso. La protección contra los accesos no autorizados se realiza mediante el filtrado de puertos y el sistema antes mencionado de llaves públicas y privadas en donde el servidor no acepta accesos mediante contraseña.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

Las plataformas son respaldadas utilizando un sistema de respaldos completo en donde se toma el código fuente y la base de datos en un proceso automatizado utilizando scripts escritos en Bash con una periodicidad variable (base de datos todos los días, código fuente cada 3, 6 o 15 días según la criticidad del proyecto). Los respaldos son almacenados de forma temporal en un servidor dedicado a ello, por un promedio de treinta días tras, y almacenado de forma permanente en una cinta magnética. Las cintas magnéticas son resguardadas por el Departamento de Operaciones y Seguridad Informática en un almacén dedicado para ello que mantiene las cintas seguras y en condiciones óptimas para su funcionamiento. Para promover la conservación y preservación de la información, las cintas y el lector de estas se mantienen por tiempo indefinido.

## **IX. PLAN DE CONTINGENCIA**

Se cuenta con un plan de contingencia que permite la continuidad de negocio, el cual utiliza como fuente primordial los respaldos obtenidos de las plataformas en cintas magnéticas y en un servidor dedicado. Las pruebas de eficiencia que se realizan han garantizado la recuperación total de la plataforma en un periodo máximo de doce horas. Actualmente no se cuenta con un sitio redundante o alternativo.

## **7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD**

### **7.1. Herramientas y recursos para monitoreo de la protección de datos personales**

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-005	
(Nombre del sistema A1) *	Resultados de Evaluación de Actividades de Formación Docente	
Recurso*	Descripción*	Control*
Bitácoras del sistema	Revisión aleatoria del contenido de los logs del sistema operativo y aplicación.	Se realiza una revisión no automatizada buscando patrones de ataque conocidos y secuencias de ataques conocidas como el descubrimiento de puertos y búsqueda de archivos de configuración conocidos.  Responsables: Oscar Escamilla González

## 7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-005	
(Nombre del sistema A1) *	Resultados de Evaluación de Actividades de Formación Docente	
Medida de seguridad*	Procedimiento*	Responsable*
Revisión de permisos.	Revisiones de permisos dentro del sistema operativo, servidor web y la aplicación.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.

Actualización del sistema operativo.	Actualización a nuevas versiones de los paquetes del sistema operativo.	Responsable: Oscar Escamilla Gonzalez. La duración es de dos horas aproximadamente.
Actualización de la aplicación.	Actualización de Framework y bibliotecas principales del CodeIgniter 4.	Responsable: Oscar Escamilla Gonzalez. La duración es de dos horas aproximadamente.

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-005	
(Nombre del sistema A1) *	Resultados de Evaluación de Actividades de Formación Docente	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Revisión de permisos.	Se cuentan con los permisos adecuados.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.
Actualización del sistema operativo.	Se cuentan con las últimas actualizaciones.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.
Actualización de la aplicación.	Se cuentan con las últimas actualizaciones.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.

### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único*	CUAIEED-DIEDCFD-005
(Nombre del sistema A1) *	Resultados de Evaluación de Actividades de Formación Docente

Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL	Realizar la renovación anual del certificado SSL.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.
Actualización de la aplicación.	Realizar el proceso de actualización de la plataforma.	Responsable: Oscar Escamilla Gonzalez. La duración es de una hora aproximadamente.

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

No se cuenta con un programa formal de capacitación

### 8.2. Programa de difusión de la protección a los datos personales (Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

No se tiene un programa de difusión de la protección a los datos personales

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único*	CUAIEED-DIEDCFD-005
(Nombre del sistema A1) *	Resultados de Evaluación de Actividades de Formación Docente



Actividad*	Descripción*	Duración*	Cobertura*
<i>Actualización de la plataforma a nuevas versiones.</i>	<i>Proceso de actualización con parches de seguridad de CodeIgniter 4.</i>	<i>1 mes.</i>	<i>Total.</i>

### 9.2. Actualización y mantenimiento de equipo de cómputo

Dirección de Desarrollo de Sistemas para la Educación			
<b>Identificador único*</b>	CUAIEED-DIEDCFD-005		
<b>(Nombre del sistema A1*:</b>	Resultados de Evaluación de Actividades de Formación Docente		
Actividad*	Descripción*	Duración*	Cobertura*
<i>Reparación o reemplazo del servidor (hardware)</i>	<i>Reparación o reemplazo del servidor en caso de fallo</i>	<i>Por evento</i>	<i>Total</i>

### 9.3. Procesos para la conservación, preservación y respaldos de información

Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente		
<b>Identificador único*</b>	CUAIEED-DIEDCFD-005	
<b>(Nombre del sistema A1*:</b>	Resultados de Evaluación de Actividades de Formación Docente	
Proceso*	Descripción*	Responsable*

<i>Resguardo de cintas magnéticas.</i>	<i>Las cintas magnéticas realizadas en la fase de respaldo automatizado y el lector de las cintas magnéticas son resguardadas de forma indefinida.</i>	<i>Departamento de Operaciones y Seguridad Informática.</i>
--	--	---

#### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

<b>Dirección Innovación Educativa, Desarrollo Curricular y Formación Docente</b>		
<b>Identificador único*</b>	CUAIEED-DIEDCFD-005	
<b>(Nombre del sistema A1*:</b>	Resultados de Evaluación de Actividades de Formación Docente	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
<i>Borrado seguro.</i>	<i>Se realiza un formato de bajo nivel al disco duro físico del hipervisor.</i>	<i>Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.</i>

### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El director de la Dirección de Desarrollo de Sistemas para la Educación recibe o envía la petición en donde se indica la razón para la cancelación del sistema, el tiempo que deberá de permanecer la plataforma funcionando antes de ser eliminada y si se necesita entregar un respaldo final del sistema para su resguardo final en un soporte electrónico. La petición siempre es en formato escrito ya sea por correo electrónico o por oficio. El sistema será eliminado tras una fecha de término establecida y se borra de forma permanente la máquina virtual donde este reside.

#### **Sistema de Encuesta de Formación Docente**

##### **Introducción**

El Sistema de Encuesta de Formación Docente permite la recopilación anual de información por parte de las dependencias de la UNAM que realizan actividades de formación docente con respecto a diferentes aspectos relacionados con dichas actividades y las personas involucradas en la gestión,

implementación, impartición y evaluación de estas. El sistema está compuesto por una WebApp reactiva que consume una API propia para el acceso y guardado de registros en una base de datos. El acceso al sistema sólo está disponible una pequeña temporada cada año.

## 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente</b>	
<b>Identificador único*</b>	CUAIEED-DIEDCFD-006
<b>Nombre del sistema A1*:</b>	<b>Sistema de Encuesta de Formación Docente</b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	Nombre, correo electrónico (personal o institucional), número de trabajador, institución de procedencia, IP
<b>Responsable*:</b>	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
<b>Nombre*:</b>	Dra. <a href="#">Ruth Torres Carrasco</a>
<b>Cargo*:</b>	Subdirección del Centro de Formación y Profesionalización para el Desarrollo Académico
<b>Funciones*:</b>	Elaboración de plataformas, materiales y apoyos didácticos multimedia que utilicen la tecnología con enfoques innovadores Elaboración de sistemas académico-administrativos para el apoyo de las actividades de formación docente Impartición de cursos, talleres y diplomados
<b>Obligaciones*:</b>	<ul style="list-style-type: none"> <li>- Definir junto con los usuarios del sistema, los tipos de acceso.</li> <li>- Vigilar que el sistema cumpla con todas las medidas de seguridad técnicas, físicas y administrativas.</li> <li>- Vigilar que los sistemas operen de manera adecuado y apegados a su propósito</li> <li>- Vigilar el correcto tratamiento y resguardo de los datos personales almacenados</li> </ul>
	<b>Encargados:</b>
<b>(Nombre del Encargado 1*):</b>	Ing. <a href="#">Carlos Alberto Jaimes Vergara</a>
<b>Cargo*:</b>	Coordinador de Formación Digital y Recursos Audiovisuales para la Docencia

<b>Funciones*:</b>	Asegurar el correcto funcionamiento del sistema, agregar nuevas funcionalidades en una dinámica de mejora continua.
<b>Obligaciones*:</b>	Proteger el software y la base de datos, así como llevar a cabo los procesos de actualización anual del sistema. Monitorear el comportamiento del sistema Procurar la protección de los datos personales contenidos en el sistema.

<b>(Nombre del Encargado 1*):</b>	Mtro. <a href="#">Guillermo Martínez Cuevas</a>
<b>Cargo*:</b>	Coordinador de Formación Docente
<b>Funciones*:</b>	Analizar los datos y representar sus resultados en un informe anual.
<b>Obligaciones*:</b>	Procurar la protección de los datos personales contenidos en el sistema.

<b>(Nombre del Encargado 1*):</b>	Mtro. Oscar Escamilla González
<b>Cargo*:</b>	Jefe de departamento de desarrollos digitales para la formación docente
<b>Funciones*:</b>	Analizar los datos y representar sus resultados en un informe anual.
<b>Obligaciones*:</b>	Procurar la protección de los datos personales contenidos en el sistema y como resultado del análisis de estos.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

<b>Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente</b>	
<b>Identificador único*</b>	CUAIEED-DIEDCFD-006
<b>(Nombre del sistema A1*)</b>	<b>Sistema de Encuesta de Formación Docente</b>
<b>Tipo de soporte: *</b>	Electrónico
<b>Descripción: *</b>	Sistema web back end + web app front end + Base de datos

### 3. ANÁLISIS DE RIESGOS

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente		
Identificador único	CUAIEED-DIEDCFD-006	
Nombre del sistema A1)	Sistema de Encuesta de Formación Docente	
Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado.	Alto	Uso de contraseñas seguras, cifrado de comunicaciones entre el cliente y el servidor. Cambio de credenciales cada periodo de apertura del sistema
Acceso Directo a registros de la base de datos	Alto	Cifrado de datos. Separación de back end en otro servidor web con acceso al servicio sólo desde la ip del cliente o front end

### 4. ANÁLISIS DE BRECHA

Identificador único*	CUAIEED-DIEDCFD-006	
Nombre del sistema A1) *	Sistema de Encuesta de Formación Docente	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Acceso a base de datos sólo desde una IP específica dentro del centro de datos y a través de un túnel cifrado con SSH. El acceso HTTPS sólo recibe respuesta del back end si se hace la petición desde la IP del cliente permitido	Registros de datos cifrados	Desarrollo de cifrado de datos desde el sistema
Accesos a través de contraseñas seguras y sesiones respaldadas por JWT	Versión Actualizada de JWT	Actualizar nuevas versiones tokens web JSON

## 5. PLAN DE TRABAJO

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente			
Identificador único*	CUAIEED-DIEDCFD-006		
(Nombre del sistema A1) *	Sistema de Encuesta de Formación Docente		
Actividad*	Descripción*	Duración*	Cobertura*
Desarrollo de cifrado de datos desde el sistema	Diseñar e implementar proceso de cifrado y descifrado de todos los datos contenidos en la actual Base de datos, de tal modo que, aunque un usuario malintencionado tuviera	3 semanas	Total

acceso a la base, no pueda descifrarlos

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente	
Identificador único*	CUAIEED-DIEDCFD-006
(Nombre del sistema A1) *	Sistema de Encuesta de Formación Docente
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
Transferencias mediante el traslado de soportes físicos:	No se realiza tratamiento de datos personales con soportes físicos, se tiene soporte electrónico en una base de datos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de datos entre sistemas front end y back end se dan de manera cifrada y la conexión se da de manera exclusiva entre las partes vía whitelist de IP y rutas de acceso y métodos específicos, además de directivas CORS.

### I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No aplica, se tiene soporte electrónico en una base de datos.

### II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras se almacenan en formato electrónico en archivos de log dentro del servidor web y la base de datos del Sistema de Encuesta de Formación Docente, almacenando la fecha, hora, dirección IP, así como todas las acciones dentro del sistema. Los archivos de log que se encuentran dentro del sistema operativo se rotan cada semana.

### III. REGISTRO DE INCIDENTES

Los incidentes son reportados a los encargados de infraestructura de la Unidad de Sistemas en donde se realiza un análisis de logs del sistema operativo y las bitácoras del aplicativo para determinar la

gravedad de la incidencia. Se cuenta con dos métodos de recuperación de los datos: utilizando un respaldo completo o recuperando parte de los datos comprometidos utilizando técnicas forenses.

La base de datos es respaldada diariamente y son rotadas cada 15 días, por su parte el backend y frontend del aplicativo se encuentra en un repositorio GIT privado y puede ser recuperada cualquier versión del sistema.

## **V. ACCESO A LAS INSTALACIONES**

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente. La dependencia se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar).

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

El procedimiento para actualizar o corregir datos personales se realiza directamente con la encargada del área operativa de Formación Docente, indicando previamente que los datos resguardados son transferidos directamente de los registros de la Dirección General de Personal, por lo que es muy raro que se requieran actualizaciones, sin embargo, las actualizaciones que competan directamente al alcance del sistema se realizarán en un plazo no mayor a cuarenta y ocho horas tras ser recibida la solicitud en horario y días laborables.

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

El número de usuarios del sistema es 52, ninguno de ellos tiene acceso a los datos personales, cada usuario captura sus propios datos, por medio de credenciales previamente creadas y sólo para este propósito. Cada usuario es designado por el director de cada una de las dependencias de la Universidad en donde se llevan a cabo actividades de formación docente. El análisis de datos se da con una extracción vía consultas en la base de datos para luego ser procesados en Power BI.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

Se cuenta con un esquema de respaldo diario tanto del sistema, la configuración middleware y del servidor, además de la base de datos, con una rotación cada 15 días naturales, además el sistema backend y frontend están resguardados en un repositorio GIT privado.

## **IX. PLAN DE CONTINGENCIA**

Se cuenta con un plan de contingencia que permite la continuidad de negocio, el cual utiliza como fuente de datos los últimos respaldos montados en un servidor virtual dedicado. La recuperación total del sistema puede ser llevada en un periodo máximo de 36 horas. Actualmente no se cuenta con un sitio redundante o alternativo.

## **7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD**



## 7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-006	
Nombre del sistema A1) *	Sistema de Encuesta de Formación Docente	
Recurso*	Descripción*	Control*
Bitácoras del sistema	Revisión aleatoria del contenido de los logs del sistema operativo y aplicación.	Se realiza una revisión no automatizada buscando patrones de ataque conocidos y secuencias de ataques conocidas como el descubrimiento de puertos y búsqueda de archivos de configuración conocidos.

## 7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-006	
Nombre del sistema A1) *	Sistema de Encuesta de Formación Docente	
Medida de seguridad*	Procedimiento*	Responsable*
Script de respaldo de información.	Revisión aleatoria del contenido de los respaldos realizados.	Responsable: Coordinación de formación Digital y Recursos Audiovisuales para la Docencia
Actualización de la aplicación.	Actualización de componentes principales del Sistema de Encuesta de Formación Docente.	Responsable: Coordinación de formación Digital y Recursos Audiovisuales para la Docencia

### 7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-006	
Nombre del sistema A1) *	Sistema de Encuesta de Formación Docente	
Medida de seguridad*	Resultado de evaluación*	Responsable*
No pasó por Revisión Cert UNAM, sin embargo, se siguieron sus recomendaciones de seguridad en su desarrollo.		Responsable: Coordinación de formación Digital y Recursos Audiovisuales para la Docencia

### 7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente		
Identificador único*	CUAIEED-DIEDCFD-006	
Nombre del sistema A1) *	Sistema de Encuesta de Formación Docente	
Medida de seguridad*	Acciones*	Responsable*
Uso de certificados SSL.	Realizar la renovación periódica del certificado SSL.	Responsable: Coordinación de formación Digital y Recursos Audiovisuales para la Docencia
Actualización del Sistema de Encuesta de Formación Docente.	Realizar el proceso de actualización del sistema.	Responsable: Coordinación de formación Digital y Recursos Audiovisuales para la Docencia

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

### 8.1. Programa de capacitación a los responsables de seguridad de datos personales

No se cuenta con un programa formal de capacitación

### 8.2. Programa de difusión de la protección a los datos personales

(Llenar una tabla para cada sistema. Campos con \* son obligatorios. Borrar instrucciones en cursivas)

No se tiene un programa de difusión de la protección a los datos personales

## 9. MEJORA CONTINUA

### 9.1. Actualización y mantenimiento de sistemas de información

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente			
Identificador único*	CUAIEED-DIEDCFD-006		
(Nombre del sistema A1) *	Sistema de Encuesta de Formación Docente		
Actividad*	Descripción*	Duración*	Cobertura*
<i>Actualización del Sistema de Encuesta de Formación Docente.</i>	<i>Realizar el proceso de actualización del sistema.</i>	<i>Periódica.</i>	<i>Parcial e incremental</i>

### 9.2. Actualización y mantenimiento de equipo de cómputo

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente	
Identificador único*	CUAIEED-DIEDCFD-006
(Nombre del sistema A1*:	Sistema de Encuesta de Formación Docente

Actividad*	Descripción*	Duración*	Cobertura*
Actualización del servidor físico.	<i>Cambio del servidor físico utilizado para crear máquinas virtuales donde se hospeda el Sistema de Encuesta de Formación Docente.</i>	3 años.	Total.

### 9.3. Procesos para la conservación, preservación y respaldos de información

(Denominación del área específica del Área Universitaria A) *		
Identificador único*	CUAIEED-DIEDCFD-006	
(Nombre del sistema A1*:	Sistema de Encuesta de Formación Docente	
Proceso*	Descripción*	Responsable*
Resguardo de cintas magnéticas.	<i>Las cintas magnéticas realizadas en la fase de respaldo automatizado y el lector de las cintas magnéticas son resguardadas de forma indefinida.</i>	<i>Departamento de Operaciones y Seguridad Informática.</i>

### 9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente	
Identificador único*	CUAIEED-DIEDCFD-006
(Nombre del sistema A1*:	Sistema de Encuesta de Formación Docente

Proceso*	Descripción*	Responsable*
Borrado seguro.	Se realiza un formato de bajo nivel al disco duro físico del hipervisor.	Responsable: Departamento de Operaciones y Seguridad Informática. Tiempo máximo de 24 horas.

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La Dirección De Innovación Educativa, Desarrollo Curricular Y Formación Docente recibe o envía la petición en donde se indica la razón para la cancelación del sistema, el tiempo que deberá de permanecer la plataforma funcionando antes de ser eliminada y si se necesita entregar un respaldo final del sistema para su resguardo final en un soporte electrónico. La petición siempre es en formato escrito ya sea por correo electrónico o por oficio. El sistema será eliminado tras una fecha de término establecida y se borra de forma permanente la máquina virtual donde este reside.

### Sistema Integral de Gestión de Exámenes (SIGE)

#### Introducción

El SIGE es una herramienta que permite gestionar el proceso de generación de exámenes; cuenta con 4 perfiles de usuario, cada uno de ellos con privilegios específicos sobre la información alojada en el sistema. El sistema cuenta con múltiples reportes descargables para facilitar los procesos de las diferentes áreas que lo utilizan.

#### 1. INVENTARIO

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-001
Nombre del sistema	Sistema Integral de Gestión de Exámenes (SIGE)
Datos personales contenidos en el sistema <sup>3</sup> para los roles de usuario: <ul style="list-style-type: none"> <li>● Responsable del sistema</li> <li>● Responsable de programa</li> <li>● Responsable de asignatura</li> <li>● Responsable de calibración</li> </ul>	<ul style="list-style-type: none"> <li>● Nombre</li> <li>● Apellido Paterno</li> <li>● Apellido Materno</li> <li>● Correo electrónico</li> </ul>
Responsable:	Dirección de Evaluación Educativa
Nombre:	Dr. Adrián Martínez
Cargo:	Director de Evaluación Educativa
Funciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones:	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
Encargados	
Nombre de Encargado 1	Mtra. Nancy Sofía Contreras Michel

<sup>3</sup> Todos los usuarios registrados en el sistema firman una carta de confidencialidad

Cargo	Subdirectora de Evaluación de Posgrado y Titulación
Funciones	Brindar seguimiento a los procesos de registro de usuarios.
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 2	Lic. Enrique Ricardo Buzo Casanova
Cargo	Subdirector de Evaluación de Bachillerato y Licenciatura
Funciones	Brindar seguimiento a los procesos de registro de usuarios.
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 3	Ing. Milton Arturo García Lima
Cargo	Jefe de la Unidad de Sistemas para la Evaluación Educativa
Funciones	Realizar el proceso de software (formularios de datos personales para el registro de usuarios) con la finalidad de atender las necesidades administrativas de la DEE garantizando que la información almacenada es veraz, oportuna y confiable
Obligaciones	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
Nombre de Encargado 4	Lic. Isaac Aboytes Morales
Cargo	Jefe de Departamento de Plataformas de Exámenes
Funciones	Realizar procesos de respaldo y restauración de la información contenida en el sistema
Obligaciones	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad (control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
<b>Usuarios</b>	
Tipo de usuario	Descripción
Responsable general	Personal autorizado de la CUAIEED
Responsable de programa	Personal autorizado de la CUAIEED
Responsable de asignatura	Personal autorizado de la CUAIEED
Responsable de calibración	Personal autorizado de la CUAIEED

## 2. ESTRUCTURA Y DESCRIPCIÓN

<b>Dirección de Evaluación Educativa</b>	
Identificador único	CUAIEED-DEE-001
Nombre del sistema	Sistema Integral de Gestión de Exámenes (SIGE)
Tipo de soporte <sup>4</sup>	Electrónico
Descripción <sup>5</sup>	Base de datos relacional
Características del lugar donde se resguardan los soportes	Información reservada El centro de datos (versión privada) es una habitación reservada para los servidores, cuenta con sistema de enfriamiento y redundancia de alimentación eléctrica.

<sup>4</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

<sup>5</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

<sup>6</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros)

	<p>Se cuenta con una intranet donde están los equipos de trabajo de los usuarios que utilizan el sistema y manipulan la información.</p> <p>El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso. Se cuenta con circuito cerrado que graba los movimientos.</p>
--	---

### 3. ANÁLISIS DE RIESGOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-001	
Nombre del sistema	Sistema Integral de Gestión de Exámenes (SIGE)	
Riesgo	Impacto	Mitigación
Datos de acceso comprometidos	Alto	Renovar claves de acceso, emitir cartas de confidencialidad y compartir con los responsables de la información para actualizar el expediente
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso, emitir cartas de confidencialidad y compartir con los responsables de la información para actualizar el expediente
Virus informático	Alto	Instalación de antivirus. Actualización constante del antivirus. Eliminar amenaza en el equipo comprometido. Plan de respaldo y recuperación
Ataque informático	Alto	Identificar y solucionar amenaza(s) y vulnerabilidad(es). Plan de respaldo y recuperación
Pérdida de información	Alto	Plan de respaldo y recuperación
Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos  Lógico: revisión periódica de servicios y puertos habilitados  Monitoreo: <ul style="list-style-type: none"> <li>• Sistema de cámaras de circuito cerrado</li> <li>• Sistema de detección de intrusos</li> </ul>
Suministro e instalación eléctrica		
CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado
Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros	Alto	Se cuenta con un plan de respaldo y recuperación de información

### 4. ANÁLISIS DE BRECHA

del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-001	
Nombre del sistema	Sistema Integral de Gestión de Exámenes (SIGE)	
Nombre	Causa	Solución
Actualizaciones al sistema operativo	No actualizar el sistema operativo	Actualizaciones periódicas a los sistemas operativos
Actualizaciones la plataforma de desarrollo	Compatibilidad con las versiones de producción. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación
Servidores web y de aplicaciones	Compatibilidad con las versiones de producción de sistemas operativos y librerías. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación
Cuentas de acceso en desuso	Término de relación laboral del personal asignado Falta de notificación al área para realizar la restricción de acceso correspondiente	Revisión periódica de cuentas de usuarios vigentes
Asignación errónea de privilegios de usuario	Equivocación en la creación de cuentas de usuario. Solicitud de cambios en los privilegios en las cuentas de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario
Capacitación a usuarios	Falta de capacitación a usuarios que provoque la falta de confiabilidad en la integridad de la información (nuevos usuarios y/o cambios de rol de usuarios)	Capacitar adecuadamente al personal para los roles asignados
Flujo de la información	Solicitud de omisión de procesos durante el flujo de información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema

## 5. PLAN DE TRABAJO

Dirección de Evaluación Educativa				
Identificador único	CUAIEED-DEE-001			
Nombre del sistema	Sistema Integral de Gestión de Exámenes (SIGE)			
Control	Actividades por realizar	Duración	Prioridad	Áreas responsables
Actualizaciones al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones a la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa



	posterior publicación			
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-001
Nombre del sistema	Sistema Integral de Gestión de Exámenes (SIGE)
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital). Filtrado de paquetes desde y hacia el servidor web.

### II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Sistema Integral de Gestión de Exámenes genera la carta de confidencialidad para los usuarios para los elaboradores, revisores y correctores de estilo, dicha carta es firmada por el usuario y resguardada por la Subdirección de Exámenes con la que colabora.

### III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

### IV. REGISTRO DE INCIDENTES

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

## V. ACCESO A LAS INSTALACIONES

*Información reservada*

La vigilancia y el acceso físico al edificio es proporcionado por el personal de los Consejos Académicos de Área. Se cuenta con una caseta de vigilancia que registra todos los accesos para el ingreso a la Dirección de Evaluación Educativa (DEE).

Para el acceso a la DEE cuenta con un lector biométrico de huella digital, el acceso al Centro de Datos está restringido únicamente al personal autorizado de la USEE (cuenta con llave) y además tiene instalado un sistema de circuito cerrado con detección de movimiento.

## VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

## VII. PERFILES DE USUARIO Y CONTRASEÑA

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hackeos* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

## XI. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-001	
Nombre del sistema	Sistema Integral de Gestión de Exámenes (SIGE)	
Recurso	Descripción	Control
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades.  Se realiza un escaneo de puertos de manera periódica con el fin de corroborar que solo estén abiertos los puertos necesarios por la aplicación.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones.

Correo electrónico	Envío de reportes mediante correos electrónicos institucionales	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario autorizado por la DEE (archivo cifrado con protección de contraseña).
--------------------	---	--

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

## 10. MEJORA CONTINUA

No aplica

### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-001		
Nombre del sistema	Sistema Integral de Gestión de Exámenes (SIGE)		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-001		
Nombre del sistema	Sistema Integral de Gestión de Exámenes (SIGE)		
Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-001	
Nombre del sistema	Sistema Integral de Gestión de Exámenes (SIGE)	
Proceso	Descripción	Responsable
Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los respaldos automatizados se resguardan de manera indefinida	Unidad de Sistemas para la Evaluación Educativa (USEE)

## 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-001	
Nombre del sistema	Sistema Integral de Gestión de Exámenes (SIGE)	
Proceso	Descripción	Responsable
Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa. El sistema será eliminado una vez expirado el tiempo solicitado. por medio de requerimiento.

### Repositorio Digital

#### Introducción

El Repositorio Digital es una herramienta que permite controlar el proceso de elaboración de reactivos con base en criterios de calidad específicos. El Repositorio Digital tiene tres perfiles de usuario y cada uno de ellos cuenta con privilegios específicos sobre la información alojada en el sistema.

#### 1. INVENTARIO

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-002
Nombre del sistema	Repositorio Digital
Datos personales contenidos en el sistema <sup>7</sup> para los roles de usuario: <ul style="list-style-type: none"> <li>● Elaborador de reactivos</li> <li>● Revisor de reactivos</li> <li>● Corrector de estilo</li> </ul>	<ul style="list-style-type: none"> <li>● Nombre</li> <li>● Apellido Paterno</li> <li>● Apellido Materno</li> <li>● Correo electrónico</li> <li>● RFC</li> <li>● Teléfono</li> <li>● Dirección (incluye Calle, Colonia, Delegación o municipio, Código postal, Estado, Ciudad)</li> <li>● Grado de estudios</li> <li>● Nombramiento</li> </ul>
<b>Responsable:</b>	<b>Dirección de Evaluación Educativa</b>
Nombre:	Dr. Adrián Martínez
Cargo:	Director de Evaluación Educativa
Funciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones:	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.

<sup>7</sup> Todos los usuarios registrados en el sistema firman una carta de confidencialidad

Encargados	
Nombre de Encargado 1	Mtra. Nancy Sofía Contreras Michel
Cargo	Subdirectora de Evaluación de Posgrado y Titulación
Funciones	Brindar seguimiento a los procesos de registro de usuarios.
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 2	Lic. Enrique Ricardo Buzo Casanova
Cargo	Subdirector de Evaluación de Bachillerato y Licenciatura
Funciones	Brindar seguimiento a los procesos de registro de usuarios.
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 3	Ing. Milton Arturo García Lima
Cargo	Jefe de la Unidad de Sistemas para la Evaluación Educativa
Funciones	Realizar el proceso de software (formularios de datos personales para el registro de usuarios) con la finalidad de atender las necesidades administrativas de la DEE garantizando que la información almacenada es veraz, oportuna y confiable
Obligaciones	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
Nombre de Encargado 4	Lic. Isaac Aboytes Morales
Cargo	Jefe de Departamento de Plataformas de Exámenes
Funciones	Realizar procesos de respaldo y restauración de la información contenida en el sistema
Obligaciones	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad (control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
Usuarios	
Tipo de usuario	
Elaborador de reactivos	Docentes y académicos de la UNAM
Revisor de reactivos	Docentes y académicos de la UNAM
Corrector de estilo	Docentes y académicos de la UNAM

## 2. ESTRUCTURA Y DESCRIPCIÓN

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-002
Nombre del sistema	Repositorio Digital
Tipo de soporte <sup>8</sup>	Electrónico
Descripción <sup>9</sup>	Base de datos relacional

<sup>8</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

<sup>9</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

Características del lugar donde se resguardan los soportes	El centro de datos (versión privada <sup>10</sup> ) es una habitación reservada para los servidores, cuenta con sistema de enfriamiento y redundancia de alimentación eléctrica. El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso. Se cuenta con circuito cerrado que graba los movimientos.
--	--

### 3. ANÁLISIS DE RIESGOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-002	
Nombre del sistema	Repositorio Digital	
Riesgo	Impacto	Mitigación
Datos de acceso comprometidos	Alto	Renovar claves de acceso, emitir cartas de confidencialidad y compartir con los responsables de la información para actualizar el expediente
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso, emitir cartas de confidencialidad y compartir con los responsables de la información para actualizar el expediente
Virus informático	Alto	Instalación de antivirus. Actualización constante del antivirus. Eliminar amenaza en el equipo comprometido. Plan de respaldo y recuperación.
Ataque informático	Alto	Identificar y solucionar amenaza(s) y vulnerabilidad(es). Plan de respaldo y recuperación.
Pérdida de información	Alto	Plan de respaldo y recuperación.
Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos.  Lógico: revisión periódica de servicios y puertos habilitados.  Monitoreo: <ul style="list-style-type: none"> <li>• Sistema de cámaras de circuito cerrado</li> <li>• Sistema de detección de intrusos</li> </ul>
Suministro e instalación eléctrica		
CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado

<sup>10</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros	Alto	Se cuenta con un plan de respaldo y recuperación de información

#### 4. ANÁLISIS DE BRECHA

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-002	
Nombre del sistema	Repositorio Digital	
Nombre	Causa	Solución
Actualizaciones al sistema operativo	No actualizar el sistema operativo	Actualizaciones periódicas a los sistemas operativos
Actualizaciones a la plataforma de desarrollo	Compatibilidad con las versiones de producción. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación
Servidores web y de aplicaciones	Compatibilidad con las versiones de producción de sistemas operativos y librerías. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación
Cuentas de acceso en desuso	Término de relación laboral del personal asignado Falta de notificación al área para realizar la restricción de acceso correspondiente	Revisión periódica de cuentas de usuarios vigentes
Asignación errónea de privilegios de usuario	Equivocación en la creación de cuentas de usuario Solicitud de cambios en los privilegios en las cuentas de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario
Capacitación a usuarios	Falta de capacitación a usuarios que provoque la falta de confiabilidad en la integridad de la información (nuevos usuarios y/o cambios de rol de usuarios)	Capacitar adecuadamente al personal para los roles asignados
Flujo de la información	Solicitud de omisión de procesos durante el flujo de información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema

#### 5. PLAN DE TRABAJO

Dirección de Evaluación Educativa				
Identificador único	CUAIEED-DEE-002			
Nombre del sistema	Repositorio Digital			
Control	Actividades por realizar	Duración	Prioridad	Áreas responsables

Actualizaciones al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones a la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-002
Nombre del sistema	Repositorio Digital
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital). Filtrado de paquetes desde y hacia el servidor web.

### II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS



El Repositorio Digital no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

### III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

### IV. REGISTRO DE INCIDENTES

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

### V. ACCESO A LAS INSTALACIONES

La vigilancia y el acceso físico al edificio es proporcionado por el personal de los Consejos Académicos de Área. Se cuenta con una caseta de vigilancia que registra todos los accesos para el ingreso a la Dirección de Evaluación Educativa (DEE).  
Para el acceso a la DEE cuenta con un lector biométrico de huella digital, el acceso al Centro de Datos está restringido únicamente al personal autorizado de la USEE (cuenta con llave) y además tiene instalado un sistema de circuito cerrado con detección de movimiento.

### VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

### VII. PERFILES DE USUARIO Y CONTRASEÑA

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hackeos* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

### VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

### XI. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

### 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Dirección de Evaluación Educativa		
Identificador único	QUAIEED-DEE-002	
Nombre del sistema	Repositorio Digital	
Recurso	Descripción	Control
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades.

	escaneo de puertos abiertos	Se realiza un escaneo de puertos de manera periódica con el fin de corroborar que solo estén abiertos los puertos necesarios por la aplicación.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones.
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario autorizado por la DEE (archivo cifrado con protección de contraseña).

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

## 9. MEJORA CONTINUA

No aplica.

### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-002		
Nombre del sistema	Repositorio Digital		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-002		
Nombre del sistema	Repositorio Digital		
Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-002	
Nombre del sistema	Repositorio Digital	
Proceso	Descripción	Responsable
Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los	Unidad de Sistemas para la Evaluación Educativa (USEE)

	respaldos automatizados se resguardan de manera indefinida	
--	--	--

#### 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-002	
Nombre del sistema	Repositorio Digital	
Proceso	Descripción	Responsable
Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)

#### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa. El sistema será eliminado una vez expirado el tiempo solicitado por medio de requerimiento.

#### Sistema de Aprendizaje de Bachillerato en RED (SABER)

##### Introducción

El Sistema de Aprendizaje para Bachillerato En Red (SABER) permite fortalecer el conocimiento de diferentes asignaturas con ayuda de lecciones interactivas, preguntas de autoevaluación y exámenes de diagnóstico. El SABER cuenta con tres perfiles de usuario y cada uno de ellos posee privilegios específicos sobre la información alojada en el sistema. 1) Alumnos de la UNAM: Pueden resolver exámenes diagnósticos y consultar resultados, además el sistema les permite estudiar lecciones interactivas distintas asignaturas y responder preguntas de autoevaluación. 2) Profesores de la UNAM: Pueden consultar temarios, crear exámenes y programar sus aplicaciones, dar por finalizadas las aplicaciones y generar reportes de cada una de ellas, así como desbloquear a los alumnos del sistema. Además, cuentan con un módulo de autoevaluación, donde sólo pueden ver las lecciones interactivas a las que tienen acceso los Alumnos de la UNAM. 3) Público en General: Este perfil puede estudiar lecciones interactivas y responder preguntas de autoevaluación de cada asignatura.

#### 1. INVENTARIO

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-003
Nombre del sistema	Sistema de Aprendizaje de Bachillerato en Red
Datos personales contenidos en el sistema	<ul style="list-style-type: none"> <li>● Nombre</li> <li>● Apellido Paterno</li> <li>● Apellido Materno **</li> <li>● Género</li> </ul>
<ul style="list-style-type: none"> <li>● Alumnos de la UNAM *</li> </ul>	<ul style="list-style-type: none"> <li>● Número de cuenta</li> <li>● Fecha de nacimiento</li> <li>● Subsistema de bachillerato</li> </ul>

	<ul style="list-style-type: none"> <li>● Plantel</li> </ul>
<p>* La información es proporcionada por DGAE para actualizar la matrícula de alumnos registrados en cada inicio de ciclo escolar</p> <p>** Información opcional</p>	
<ul style="list-style-type: none"> <li>● Profesores de la UNAM</li> </ul>	<ul style="list-style-type: none"> <li>● No. De trabajador</li> <li>● RFC</li> <li>● Subsistema de bachillerato</li> <li>● Plantel</li> <li>● Correo electrónico</li> </ul>
<ul style="list-style-type: none"> <li>● Público en General</li> </ul>	<ul style="list-style-type: none"> <li>● Fecha de nacimiento</li> <li>● Correo electrónico</li> <li>● Estado o País de residencia</li> <li>● Nacionalidad</li> <li>● Nivel de estudios</li> <li>● Institución de procedencia</li> </ul>
<b>Responsable:</b>	
<b>Nombre:</b>	<b>Dirección de Evaluación Educativa</b>
<b>Cargo:</b>	Dr. Adrián Martínez
<b>Funciones:</b>	Director de Evaluación Educativa
<b>Obligaciones:</b>	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
<b>Obligaciones:</b>	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>Encargados</b>	
<b>Nombre de Encargado 2</b>	Lic. Enrique Ricardo Buzo Casanova
<b>Cargo</b>	Subdirector de Evaluación de Bachillerato y Licenciatura
<b>Funciones</b>	Brindar seguimiento a los procesos de registro de usuarios (oficio para obtener la base actualizada de la matrícula de alumnos de DGAE)
<b>Obligaciones</b>	Cumplir con la obligación legal de resguardar los datos personales
<b>Nombre de Encargado 3</b>	Ing. Milton Arturo García Lima
<b>Cargo</b>	Jefe de la Unidad de Sistemas para la Evaluación Educativa
<b>Funciones</b>	Realizar el proceso de software (formularios de datos personales para el registro de profesores y usuarios invitados/público en general) con la finalidad de atender las necesidades administrativas de la DEE garantizando que la información almacenada es veraz, oportuna y confiable
<b>Obligaciones</b>	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
<b>Nombre de Encargado 4</b>	Lic. Isaac Aboytes Morales
<b>Cargo</b>	Jefe de Departamento de Plataformas de Exámenes
<b>Funciones</b>	Realizar procesos de respaldo y restauración de la información contenida en el sistema
<b>Obligaciones</b>	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad (control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
<b>Usuarios</b>	
<b>Alumnos</b>	Alumnos de la comunidad UNAM

Profesores	Docentes y académicos de la UNAM
Público en general	Invitados

## 2. ESTRUCTURA Y DESCRIPCIÓN

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-003
Nombre del sistema	Sistema de Aprendizaje de Bachillerato en Red
Tipo de soporte <sup>11</sup>	Electrónico
Descripción <sup>12</sup>	Base de datos relacional
Características del lugar donde se resguardan los soportes	El centro de datos (versión privada <sup>13</sup> ) es una habitación reservada para los servidores, cuenta con sistema de enfriamiento y redundancia de alimentación eléctrica. El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso. Se cuenta con circuito cerrado que graba los movimientos.

## 3. ANÁLISIS DE RIESGOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-003	
Nombre del sistema	Sistema de Aprendizaje de Bachillerato en Red	
Riesgo	Impacto	Mitigación
Informático		
Datos de acceso comprometidos	Alto	Renovar claves de acceso
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso
Virus informático	Alto	Instalación de antivirus. Actualización constante del antivirus. Eliminar amenaza en el equipo comprometido. Plan de respaldo y recuperación
Ataque informático	Alto	Identificar y solucionar amenaza(s) y vulnerabilidad(es). Plan de respaldo y recuperación
Pérdida de información	Alto	Plan de respaldo y recuperación

<sup>11</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

<sup>12</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

<sup>13</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos  Lógico: revisión periódica de servicios y puertos habilitados  Monitoreo: <ul style="list-style-type: none"> <li>Sistema de cámaras de circuito cerrado</li> <li>Sistema de detección de intrusos</li> </ul>
Suministro e instalación eléctrica		
CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado
Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros	Alto	Se cuenta con un plan de respaldo y recuperación de información

#### 4. ANÁLISIS DE BRECHA

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-003	
Nombre del sistema	Sistema de Aprendizaje de Bachillerato en Red	
Nombre	Causa	Solución
Actualizaciones al sistema operativo	No actualizar el sistema operativo	Actualizaciones periódicas a los sistemas operativos
Actualizaciones la plataforma de desarrollo	Compatibilidad con las versiones de producción. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación
Servidores web y de aplicaciones	Compatibilidad con las versiones de producción de sistemas operativos y librerías. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación
Cuentas de acceso en desuso	Término de relación laboral del personal asignado Falta de notificación al área para realizar la restricción de acceso correspondiente	Revisión periódica de cuentas de usuarios vigentes
Asignación errónea de privilegios de usuario	Equivocación en la creación de cuentas de usuario. Solicitud de cambios en los privilegios en las cuentas de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario
Capacitación a usuarios	Falta de capacitación a usuarios que provoque la falta de confiabilidad en la integridad de la información	Capacitar adecuadamente al personal para los roles asignados

	(nuevos usuarios y/o cambios de rol de usuarios)	
Flujo de la información	Solicitud de omisión de procesos durante el flujo de información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema

## 5. PLAN DE TRABAJO

Dirección de Evaluación Educativa				
Identificador único	CUAIEED-DEE-003			
Nombre del sistema	Sistema de Aprendizaje de Bachillerato en Red			
Control	Actividades por realizar	Duración	Prioridad	Áreas responsables
Actualizaciones al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones a la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

<b>Dirección de Evaluación Educativa</b>	
Identificador único	CUAIEED-DEE-003
Nombre del sistema	Sistema de Aprendizaje de Bachillerato en Red
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital). Filtrado de paquetes desde y hacia el servidor web.

## **II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

El Sistema de Aprendizaje de Bachillerato en Red (SABER) genera informe(s) que contiene(n) datos personales del usuario (profesores, alumnos) mismos que son resguardados por el usuario responsable de la cuenta. Profesores generan informes con nombres de alumnos y números de cuenta de sus grupos de aplicación. Alumnos generan informes con datos personales propios (número de cuenta, nombre completo, plantel).

## **III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA**

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

## **IV. REGISTRO DE INCIDENTES**

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

## **V. ACCESO A LAS INSTALACIONES**

### **Información reservada**

La vigilancia y el acceso físico al edificio es proporcionado por el personal de los Consejos Académicos de Área. Se cuenta con una caseta de vigilancia que registra todos los accesos para el ingreso a la Dirección de Evaluación Educativa (DEE).

Para el acceso a la DEE cuenta con un lector biométrico de huella digital, el acceso al Centro de Datos está restringido únicamente al personal autorizado de la USEE (cuenta con llave) y además tiene instalado un sistema de circuito cerrado con detección de movimiento.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

## **VII. PERFILES DE USUARIO Y CONTRASEÑA**

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hackeos* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

## **XI. PLAN DE CONTINGENCIA**



Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-003	
Nombre del sistema	Sistema de Aprendizaje de Bachillerato en Red	
Recurso	Descripción	Control
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades.  Se realiza un escaneo de puertos de manera periódica con el fin de corroborar que solo estén abiertos los puertos necesarios por la aplicación.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones.
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario autorizado por la DEE (archivo cifrado con protección de contraseña).

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

## 9. MEJORA CONTINUA

*No aplica.*

### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-003		
Nombre del sistema	Sistema de Aprendizaje de Bachillerato en Red		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-003
Nombre del sistema	Sistema de Aprendizaje de Bachillerato en Red

Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-003	
Nombre del sistema	Sistema de Aprendizaje de Bachillerato en Red	
Proceso	Descripción	Responsable
Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los respaldos automatizados se resguardan de manera indefinida	Unidad de Sistemas para la Evaluación Educativa (USEE)

### 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-003	
Nombre del sistema	Sistema de Aprendizaje de Bachillerato en Red	
Proceso	Descripción	Responsable
Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa. El sistema será eliminado una vez expirado el tiempo solicitado por medio de requerimiento.

### **Pruébate UNAM Licenciatura**

#### Introducción

Pruébate UNAM Licenciatura es una plataforma virtual de autoevaluación y estudio que colabora con la preparación para la presentación del examen de selección a las licenciaturas de la UNAM. Cuenta con dos perfiles de usuario y cada uno de ellos posee privilegios específicos sobre la información alojada en el sistema. 1) Administrador del sistema: cuenta con los privilegios necesarios para realizar la administración de contenidos en la plataforma (reactivos, recursos y recomendaciones), activar/desactivar folios, entre otros. 2) Aspirante: tiene acceso a dos grandes módulos Práctica de exámenes (compuesto por exámenes de simulación, al finalizar cada examen conocerás el total de aciertos que hayas obtenido) y Práctica de asignatura (compuesto por nueve o diez asignaturas diferentes, cada una contiene un temario y un banco de reactivos con realimentaciones para cada respuesta, las cuales, te ayudarán a identificar los puntos débiles en tu manejo de contenidos específicos), además de contar con un módulos de apoyo como bibliografías, recursos y recomendaciones.

## 1. INVENTARIO

<b>Dirección de Evaluación Educativa</b>	
Identificador único	CUAIEED-DEE-004
Nombre del sistema	Pruébate UNAM Licenciatura
Datos personales contenidos en el sistema <ul style="list-style-type: none"> <li>• Administrador general<sup>14</sup></li> <li>• Aspirante</li> </ul>	<ul style="list-style-type: none"> <li>• Nombre</li> <li>• Apellido Paterno</li> <li>• Apellido Materno **</li> </ul>
<ul style="list-style-type: none"> <li>• Aspirante</li> </ul>	<ul style="list-style-type: none"> <li>• Nacionalidad</li> <li>• Estado</li> <li>• Fecha de nacimiento</li> <li>• Correo electrónico</li> <li>• Año de inicio de bachillerato</li> <li>• Año de término de bachillerato</li> <li>• Sistema</li> <li>• Modalidad</li> <li>• Género</li> <li>• Área</li> <li>• Carrera</li> <li>• Plantel</li> </ul>
<b>Responsable:</b>	
Nombre:	Dirección de Evaluación Educativa
Cargo:	Dr. Adrián Martínez
Funciones:	Director de Evaluación Educativa
Obligaciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>Encargados</b>	
Nombre de Encargado 2	Lic. Enrique Ricardo Buzo Casanova
Cargo	Subdirector de Evaluación de Bachillerato y Licenciatura
Funciones	Brindar seguimiento a los procesos de registro de usuarios (aspirantes)
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 3	Ing. Milton Arturo García Lima
Cargo	Jefe de la Unidad de Sistemas para la Evaluación Educativa
Funciones	Realizar el proceso de software (formularios de datos personales para el registro de aspirantes) con la finalidad de atender las necesidades administrativas de la DEE garantizando que la información almacenada es veraz, oportuna y confiable
Obligaciones	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
Nombre de Encargado 4	Lic. Isaac Aboytes Morales
Cargo	Jefe de Departamento de Plataformas de Exámenes
Funciones	Realizar procesos de respaldo y restauración de la información contenida en el sistema
Obligaciones	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad

<sup>14</sup> Todos los administradores registrados en el sistema firman una carta de confidencialidad

	(control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
Usuarios	
<b>Tipo de usuario</b>	<b>Nombre completo</b>
Administrador general	Personal autorizado por la CUAIEED
Aspirantes	Aspirantes de ingreso al nivel bachillerato de la UNAM

## 2. ESTRUCTURA Y DESCRIPCIÓN

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-004
Nombre del sistema	Pruébate UNAM Licenciatura
Tipo de soporte <sup>15</sup>	Electrónico
Descripción <sup>16</sup>	Base de datos relacional
Características del lugar donde se resguardan los soportes	El centro de datos (versión privada <sup>17</sup> ) es una habitación reservada para los servidores, cuenta con sistema de enfriamiento y redundancia de alimentación eléctrica. El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso. Se cuenta con circuito cerrado que graba los movimientos.

## 3. ANÁLISIS DE RIESGOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-004	
Nombre del sistema	Pruébate UNAM Licenciatura	
Riesgo	Impacto	Mitigación
Informático		
Datos de acceso comprometidos	Alto	Renovar claves de acceso
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso
Virus informático	Alto	Instalación de antivirus Actualización constante del antivirus

<sup>15</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

<sup>16</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

<sup>17</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

		Eliminar amenaza en el equipo comprometido. Plan de respaldo y recuperación.
Ataque informático	Alto	Identificar y solucionar amenaza(s) y vulnerabilidad(es). Plan de respaldo y recuperación.
Pérdida de información	Alto	Plan de respaldo y recuperación.
Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos  Lógico: revisión periódica de servicios y puertos habilitados  Monitoreo: <ul style="list-style-type: none"> <li>• Sistema de cámaras de circuito cerrado</li> <li>• Sistema de detección de intrusos</li> </ul>
Suministro e instalación eléctrica		
CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado
Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros.	Alto	Se cuenta con un plan de respaldo y recuperación de información

#### 4. ANÁLISIS DE BRECHA

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-004	
Nombre del sistema	Pruébate UNAM Licenciatura	
Nombre	Causa	Solución
Actualizaciones al sistema operativo	No actualizar el sistema operativo	Actualizaciones periódicas a los sistemas operativos
Actualizaciones la plataforma de desarrollo	Compatibilidad con las versiones de producción. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación
Servidores web y de aplicaciones	Compatibilidad con las versiones de producción de sistemas operativos y librerías. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación
Cuentas de acceso en desuso	Término de relación laboral del personal asignado Falta de notificación al área para realizar la restricción de acceso correspondiente	Revisión periódica de cuentas de usuarios vigentes
Asignación errónea de privilegios de usuario	Equivocación en la creación de cuentas de usuario Solicitud de cambios en los privilegios en las cuentas de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario

Capacitación a usuarios	Falta de capacitación a usuarios que provoque la falta de confiabilidad en la integridad de la información (nuevos usuarios y/o cambios de rol de usuarios)	Capacitar adecuadamente al personal para los roles asignados
Flujo de la información	Solicitud de omisión de procesos durante el flujo de información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema

## 5. PLAN DE TRABAJO

Dirección de Evaluación Educativa				
Identificador único	CUAIEED-DEE-004			
Nombre del sistema	Pruébate UNAM Licenciatura			
Control	Actividades por realizar	Duración	Prioridad	Áreas responsables
Actualizaciones al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones de la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-004
Nombre del sistema	Pruébate UNAM Licenciatura
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital). Filtrado de paquetes desde y hacia el servidor web.

### II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Pruébate UNAM Licenciatura genera informe(s) que contiene(n) datos personales del usuario (aspirantes) mismos que son resguardados por el usuario responsable de la cuenta.

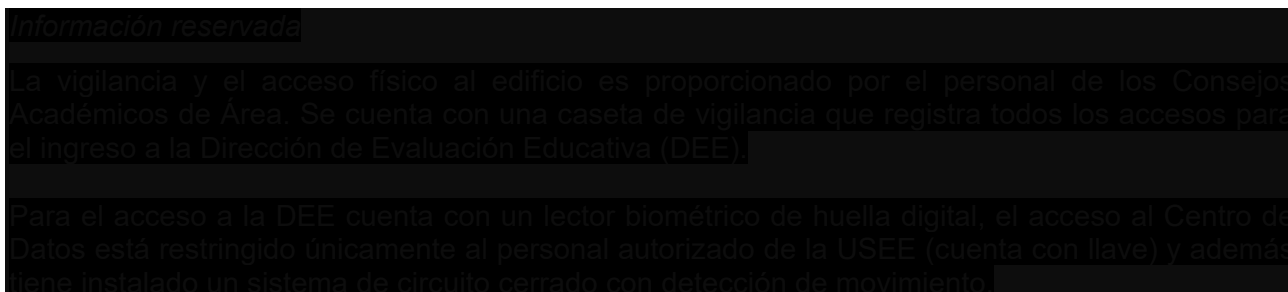
### III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

### IV. REGISTRO DE INCIDENTES

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

### V. ACCESO A LAS INSTALACIONES



### VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

### VII. PERFILES DE USUARIO Y CONTRASEÑA

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hacks* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

### VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

## XI. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

### 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-004	
Nombre del sistema	Pruébate UNAM Licenciatura	
Recurso	Descripción	Control
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades.  Se realiza un escaneo de puertos de manera periódica con el fin de corroborar que solo estén abiertos los puertos necesarios por la aplicación.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones.
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales.	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario autorizado por la DEE (archivo cifrado con protección de contraseña).

### 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

### 9. MEJORA CONTINUA

*No aplica.*

#### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-004		
Nombre del sistema	Pruébate UNAM Licenciatura		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

#### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-004



Nombre del sistema	Pruébate UNAM Licenciatura		
Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-004	
Nombre del sistema	Pruébate UNAM Licenciatura	
Proceso	Descripción	Responsable
Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los respaldos automatizados se resguardan de manera indefinida	Unidad de Sistemas para la Evaluación Educativa (USEE)

### 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-004	
Nombre del sistema	Pruébate UNAM Licenciatura	
Proceso	Descripción	Responsable
Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)

### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa. El sistema será eliminado una vez expirado el tiempo solicitado. por medio de requerimiento.

#### **Pruébate UNAM Bachillerato**

##### **Introducción**

Pruébate UNAM Bachillerato es una plataforma virtual de autoevaluación y estudio que colabora con la preparación para la presentación del examen de selección al bachillerato de la UNAM. Cuenta con dos perfiles de usuario y cada uno de ellos posee privilegios específicos sobre la información alojada en el sistema. 1) Administrador del sistema: cuenta con los privilegios necesarios para realizar la administración de contenidos en la plataforma (reactivos, recursos y recomendaciones), activar/desactivar folios, entre otros. 2) Aspirante: tiene acceso a dos grandes módulos Práctica de exámenes (compuesto por exámenes de simulación, al finalizar cada examen conocerás el total de aciertos que hayas obtenido) y Práctica de asignatura (compuesto por nueve o diez asignaturas diferentes, cada una contiene un temario y un banco de reactivos con realimentaciones para cada respuesta, las cuales, te ayudarán a identificar los puntos débiles en tu manejo de contenidos específicos), además de contar con un módulos de apoyo como bibliografías, recursos y recomendaciones.

#### **1. INVENTARIO**

<b>Dirección de Evaluación Educativa</b>	
Identificador único	CUAIEED-DEE-005
Nombre del sistema	Pruébate UNAM Bachillerato
Datos personales contenidos en el sistema <sup>18</sup> <ul style="list-style-type: none"> <li>• Administrador general</li> <li>• Aspirante</li> </ul>	<ul style="list-style-type: none"> <li>• Nombre</li> <li>• Apellido Paterno</li> <li>• Apellido Materno **</li> </ul>
<ul style="list-style-type: none"> <li>• Aspirante</li> </ul>	<ul style="list-style-type: none"> <li>• Nacionalidad</li> <li>• Estado</li> <li>• Fecha de nacimiento</li> <li>• Correo electrónico</li> <li>• Sistema</li> <li>• Modalidad</li> <li>• Género</li> </ul>
<b>Responsable:</b>	
Nombre:	Dirección de Evaluación Educativa
Cargo:	Dr. Adrián Martínez
Funciones:	Director de Evaluación Educativa
Obligaciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>Encargados</b>	
Nombre de Encargado 2	Lic. Enrique Ricardo Buzo Casanova
Cargo	Subdirector de Evaluación de Bachillerato y Licenciatura
Funciones	Brindar seguimiento a los procesos de registro de usuarios (aspirantes)
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 3	Ing. Milton Arturo García Lima
Cargo	Jefe de la Unidad de Sistemas para la Evaluación Educativa
Funciones	Realizar el proceso de software (formularios de datos personales para el registro de aspirantes) con la finalidad de atender las necesidades administrativas de la DEE garantizando que la información almacenada es veraz, oportuna y confiable
Obligaciones	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
Nombre de Encargado 4	Lic. Isaac Aboytes Morales
Cargo	Jefe de Departamento de Plataformas de Exámenes
Funciones	Realizar procesos de respaldo y restauración de la información contenida en el sistema
Obligaciones	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad (control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
<b>Usuarios</b>	
<b>Tipo de usuario</b>	<b>Nombre completo</b>

<sup>18</sup> Todos los administradores registrados en el sistema firman una carta de confidencialidad

Administrador general	Personal autorizado por la CUAIEED/DEE
Aspirantes	Aspirantes de ingreso al nivel bachillerato de la UNAM

## 2. ESTRUCTURA Y DESCRIPCIÓN

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-005
Nombre del sistema	Pruébate UNAM Bachillerato
Tipo de soporte <sup>19</sup>	Electrónico
Descripción <sup>20</sup>	Base de datos relacional
Características del lugar donde se resguardan los soportes	<p>El centro de datos (versión privada<sup>21</sup>) es una habitación reservada para los servidores, cuenta con sistema de enfriamiento y redundancia de alimentación eléctrica.</p> <p>El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso.</p> <p>Se cuenta con circuito cerrado que graba los movimientos</p>

## 3. ANÁLISIS DE RIESGOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-005	
Nombre del sistema	Pruébate UNAM Bachillerato	
Riesgo	Impacto	Mitigación
Informático		
Datos de acceso comprometidos	Alto	Renovar claves de acceso
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso
Virus informático	Alto	<p>Instalación de antivirus.</p> <p>Actualización constante del antivirus.</p> <p>Eliminar amenaza en el equipo comprometido.</p> <p>Plan de respaldo y recuperación</p>
Ataque informático	Alto	<p>Identificar y solucionar amenaza(s) y vulnerabilidad(es).</p> <p>Plan de respaldo y recuperación</p>
Pérdida de información	Alto	Plan de respaldo y recuperación

<sup>19</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

<sup>20</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

<sup>21</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos  Lógico: revisión periódica de servicios y puertos habilitados  Monitoreo: <ul style="list-style-type: none"> <li>Sistema de cámaras de circuito cerrado</li> <li>Sistema de detección de intrusos</li> </ul>
Suministro e instalación eléctrica		
CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado
Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros	Alto	Se cuenta con un plan de respaldo y recuperación de información

#### 4. ANÁLISIS DE BRECHA

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-005	
Nombre del sistema	Pruébate UNAM Bachillerato	
Nombre	Causa	Solución
Actualizaciones al sistema operativo	No actualizar el sistema operativo	Actualizaciones periódicas a los sistemas operativos
Actualizaciones la plataforma de desarrollo	Compatibilidad con las versiones de producción. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación
Servidores web y de aplicaciones	Compatibilidad con las versiones de producción de sistemas operativos y librerías. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación
Cuentas de acceso en desuso	Término de relación laboral del personal asignado Falta de notificación al área para realizar la restricción de acceso correspondiente	Revisión periódica de cuentas de usuarios vigentes
Asignación errónea de privilegios de usuario	Equivocación en la creación de cuentas de usuario. Solicitud de cambios en los privilegios en las cuentas de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario
Capacitación a usuarios	Falta de capacitación a usuarios que provoque la falta de confiabilidad en la integridad de la información	Capacitar adecuadamente al personal para los roles asignados

	(nuevos usuarios y/o cambios de rol de usuarios)	
Flujo de la información	Solicitud de omisión de procesos durante el flujo de información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema

## 5. PLAN DE TRABAJO

Dirección de Evaluación Educativa				
Identificador único		CUAIEED-DEE-005		
Nombre del sistema		Pruébate UNAM Bachillerato		
Control	Actividades por realizar	Duración	Prioridad	Áreas responsables
Actualizaciones al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones de la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-005
Nombre del sistema	Pruébate UNAM Bachillerato
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.

Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital). Filtrado de paquetes desde y hacia el servidor web.
---	--

## II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Pruébate UNAM Bachillerato genera informe(s) que contiene(n) datos personales del usuario (aspirantes) mismos que son resguardados por el usuario responsable de la cuenta.

## III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

## IV. REGISTRO DE INCIDENTES

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

## V. ACCESO A LAS INSTALACIONES

*Información reservada*

La vigilancia y el acceso físico al edificio es proporcionado por el personal de los Consejos Académicos de Área. Se cuenta con una caseta de vigilancia que registra todos los accesos para el ingreso a la Dirección de Evaluación Educativa (DEE).

Para el acceso a la DEE cuenta con un lector biométrico de huella digital, el acceso al Centro de Datos está restringido únicamente al personal autorizado de la USEE (cuenta con llave) y además tiene instalado un sistema de circuito cerrado con detección de movimiento.

## VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

## VII. PERFILES DE USUARIO Y CONTRASEÑA

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hackeos* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

## XI. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

*Dirección de Evaluación Educativa*

Identificador único	CUAIEED-DEE-005		
Nombre del sistema	Pruébate UNAM Bachillerato		
Recurso	Descripción	Control	
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades.	
		Se realiza un escaneo de puertos de manera periódica con el fin de corroborar que solo estén abiertos los puertos necesarios por la aplicación.	
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones.	
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales.	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario autorizado por la DEE (archivo cifrado con protección de contraseña).	

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

## 9. MEJORA CONTINUA

*No aplica*

### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-005		
Nombre del sistema	Pruébate UNAM Bachillerato		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-005		
Nombre del sistema	Pruébate UNAM Bachillerato		
Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-005	
Nombre del sistema	Pruébate UNAM Bachillerato	
Proceso	Descripción	Responsable
Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los respaldos automatizados se resguardan de manera indefinida	Unidad de Sistemas para la Evaluación Educativa (USEE)

### 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-005	
Nombre del sistema	Pruébate UNAM Bachillerato	
Proceso	Descripción	Responsable
Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)

### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa. El sistema será eliminado una vez expirado el tiempo solicitado. por medio de requerimiento.

#### Diseño y Aplicación de Exámenes (DAEX)

##### Introducción

Esta plataforma es una herramienta que emplea la metodología de exámenes de alto impacto de la UNAM. Ofrece asesoría especializada por medio de videos explicativos de la metodología y del uso de la plataforma, así como soporte a usuarios. Simplifica la metodología de construcción de exámenes en 4 pasos: diseñar, aplicar, analizar y almacenar; permite realizar evaluaciones formativas o sumativas y es de fácil configuración por lo que permite ahorrar tiempo. Además, es asequible, garantiza la seguridad, organización y administración de reactivos. Cuenta con un diseño web responsivo y no requiere la instalación de software adicional. Cuenta con dos perfiles de usuario y cada uno de ellos posee privilegios específicos sobre la información alojada en el sistema. 1) Profesor: crear reactivos, exámenes, programar y realizar aplicaciones en línea. 2) Alumnos: participar en las diferentes aplicaciones programadas y recibir una realimentación personalizada por el profesor.

##### 1. INVENTARIO

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-006



Nombre del sistema	Diseño y Aplicación de Exámenes (DAEX)
Datos personales contenidos en el sistema <ul style="list-style-type: none"> <li>Profesor</li> </ul>	<ul style="list-style-type: none"> <li>Número de trabajador UNAM</li> <li>RFC</li> <li>Nombre</li> <li>Apellido Paterno</li> <li>Apellido Materno **</li> <li>Correo electrónico</li> </ul>
<ul style="list-style-type: none"> <li>Aspirante</li> </ul>	<ul style="list-style-type: none"> <li>Nombre</li> <li>Apellido Paterno</li> <li>Apellido Materno **</li> <li>Género</li> <li>Fecha de nacimiento</li> <li>Correo electrónico</li> </ul>
<b>** Información opcional</b>	
<b>Responsable:</b>	
Nombre:	Dirección de Evaluación Educativa
Cargo:	Dr. Adrián Martínez
Funciones:	Director de Evaluación Educativa
Obligaciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>Encargados</b>	
Nombre de Encargado 2	Mtra. Nancy Sofía Contreras Michel
Cargo	Subdirectora de Evaluación de Posgrado y Titulación
Funciones	Brindar seguimiento a los procesos de registro de usuarios (profesores y alumnos)
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 3	Ing. Milton Arturo García Lima
Cargo	Jefe de la Unidad de Sistemas para la Evaluación Educativa
Funciones	Realizar el proceso de software (formularios de datos personales para el registro de profesores y alumnos) con la finalidad de atender las necesidades administrativas de la DEE garantizando que la información almacenada es veraz, oportuna y confiable
Obligaciones	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
Nombre de Encargado 4	Lic. Isaac Aboytes Morales
Cargo	Jefe de Departamento de Plataformas de Exámenes
Funciones	Realizar procesos de respaldo y restauración de la información contenida en el sistema
Obligaciones	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad (control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
<b>Usuarios</b>	
<b>Tipo de usuario</b>	<b>Nombre completo</b>
Profesores	Docentes y académicos de la UNAM

Alumnos	Alumnos de la comunidad UNAM
---------	------------------------------

## 2. ESTRUCTURA Y DESCRIPCIÓN

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-006
Nombre del sistema	Diseño y Aplicación de Exámenes (DAEX)
Tipo de soporte <sup>22</sup>	Electrónico
Descripción <sup>23</sup>	Base de datos relacional
Características del lugar donde se resguardan los soportes	El centro de datos (versión privada <sup>24</sup> ) es una habitación reservada para los servidores, cuenta con sistema de enfriamiento y redundancia de alimentación eléctrica. El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso. Se cuenta con circuito cerrado que graba los movimientos.

## 3. ANÁLISIS DE RIESGOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-006	
Nombre del sistema	Diseño y Aplicación de Exámenes (DAEX)	
Riesgo	Impacto	Mitigación
Informático		
Datos de acceso comprometidos	Alto	Renovar claves de acceso
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso
Virus informático	Alto	Instalación de antivirus. Actualización constante del antivirus. Eliminar amenaza en el equipo comprometido. Plan de respaldo y recuperación.
Ataque informático	Alto	Identificar y solucionar amenaza(s) y vulnerabilidad(es). Plan de respaldo y recuperación.
Pérdida de información	Alto	Plan de respaldo y recuperación.
Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos.

<sup>22</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

<sup>23</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

<sup>24</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

		Lógico: revisión periódica de servicios y puertos habilitados
		Monitoreo: <ul style="list-style-type: none"> <li>• Sistema de cámaras de circuito cerrado</li> <li>• Sistema de detección de intrusos</li> </ul>
Suministro e instalación eléctrica		
CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado
Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros	Alto	Se cuenta con un plan de respaldo y recuperación de información

#### 4. ANÁLISIS DE BRECHA

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-006	
Nombre del sistema	Diseño y Aplicación de Exámenes (DAEX)	
Nombre	Causa	Solución
Actualizaciones al sistema operativo	No actualizar el sistema operativo	Actualizaciones periódicas a los sistemas operativos
Actualizaciones la plataforma de desarrollo	Compatibilidad con las versiones de producción. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación
Servidores web y de aplicaciones	Compatibilidad con las versiones de producción de sistemas operativos y librerías. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación
Cuentas de acceso en desuso	Término de relación laboral del personal asignado Falta de notificación al área para realizar la restricción de acceso correspondiente	Revisión periódica de cuentas de usuarios vigentes
Asignación errónea de privilegios de usuario	Equivocación en la creación de cuentas de usuario Solicitud de cambios en los privilegios en las cuentas de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario
Capacitación a usuarios	Falta de capacitación a usuarios que provoque la falta de confiabilidad en la integridad de la información (nuevos usuarios y/o cambios de rol de usuarios)	Capacitar adecuadamente al personal para los roles asignados

Flujo de la información	Solicitud de omisión de procesos durante el flujo de información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema
-------------------------	--	---

## 5. PLAN DE TRABAJO

Dirección de Evaluación Educativa				
Identificador único	CUAIEED-DEE-006			
Nombre del sistema	Diseño y Aplicación de Exámenes (DAEX)			
Control	Actividades por realizar	Duración	Prioridad	Áreas responsables
Actualizaciones al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones de la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-006
Nombre del sistema	Diseño y Aplicación de Exámenes (DAEX)
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.

Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital). Filtrado de paquetes desde y hacia el servidor web.
---	--

## II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Diseño y Aplicación de Exámenes (DAEX) genera informe(s) que contiene(n) datos personales del usuario (profesores, alumnos) mismos que son resguardados por el usuario responsable de la cuenta. Profesores generan informes con nombres de alumnos y números de cuenta de sus grupos de aplicación. Alumnos generan informes con datos personales propios (número de cuenta, nombre completo, plantel).

## III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

## IV. REGISTRO DE INCIDENTES

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

## V. ACCESO A LAS INSTALACIONES

Información reservada

La vigilancia y el acceso físico al edificio es proporcionado por el personal de los Consejos Académicos de Área. Se cuenta con una caseta de vigilancia que registra todos los accesos para el ingreso a la Dirección de Evaluación Educativa (DEE).

Para el acceso a la DEE cuenta con un lector biométrico de huella digital, el acceso al Centro de Datos está restringido únicamente al personal autorizado de la USEE (cuenta con llave) y además tiene instalado un sistema de circuito cerrado con detección de movimiento.

## VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

## VII. PERFILES DE USUARIO Y CONTRASEÑA

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hackeos* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

## XI. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-006	
Nombre del sistema	Diseño y Aplicación de Exámenes (DAEX)	
Recurso	Descripción	Control
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades.  Se realiza un escaneo de puertos de manera periódica con el fin de corroborar que solo estén abiertos los puertos necesarios por la aplicación.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones.
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales.	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario autorizado por la DEE (archivo cifrado con protección de contraseña).

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

## 9. MEJORA CONTINUA

*No aplica*

### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-006		
Nombre del sistema	Diseño y Aplicación de Exámenes (DAEX)		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-006		
Nombre del sistema	Diseño y Aplicación de Exámenes (DAEX)		
Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-006	
Nombre del sistema	Diseño y Aplicación de Exámenes (DAEX)	
Proceso	Descripción	Responsable
Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los respaldos automatizados se resguardan de manera indefinida	Unidad de Sistemas para la Evaluación Educativa (USEE)

### 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-006	
Nombre del sistema	Diseño y Aplicación de Exámenes (DAEX)	
Proceso	Descripción	Responsable
Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)

### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa. El sistema será eliminado una vez expirado el tiempo solicitado. por medio de requerimiento.

#### Sistema de Análisis Psicométrico de Reactivos (SISAPRE)

##### Introducción

SISAPRE-UNAM es una plataforma destinada a apoyar a docentes e investigadores en la evaluación psicométrica de pruebas objetivas. Esta herramienta responde a la necesidad de los responsables de evaluación de contar con un software especializado que apoye sus tareas.

#### 1. INVENTARIO

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-007
Nombre del sistema	Sistema de Análisis Psicométrico de Reactivos (SISAPRE)
Datos personales contenidos en el sistema <ul style="list-style-type: none"> <li>Profesores</li> </ul>	<ul style="list-style-type: none"> <li>Número de trabajador UNAM</li> <li>RFC</li> <li>Nombre</li> <li>Apellido Paterno</li> </ul>

	<ul style="list-style-type: none"> <li>● Apellido Materno **</li> <li>● Correo electrónico</li> </ul>
<ul style="list-style-type: none"> <li>● Alumnos</li> </ul>	<ul style="list-style-type: none"> <li>● Número de cuenta</li> <li>● Nombre</li> <li>● Apellido Paterno</li> <li>● Apellido Materno **</li> <li>● Correo electrónico</li> </ul>
<ul style="list-style-type: none"> <li>● Externos</li> </ul>	<ul style="list-style-type: none"> <li>● Nombre</li> <li>● Apellido Paterno</li> <li>● Apellido Materno **</li> <li>● Correo electrónico</li> </ul>
<b>** Información opcional</b>	
<b>Responsable:</b>	<b>Dirección de Evaluación Educativa</b>
Nombre:	Dr. Adrián Martínez
Cargo:	Director de Evaluación Educativa
Funciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones:	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>Encargados</b>	
Nombre de Encargado 2	Mtro. Manuel García Minjares
Cargo	Jefe de la Coordinación Análisis de Resultados de Evaluación Educativa
Funciones	Brindar seguimiento a los procesos de registro de usuarios (profesores, alumnos y externos)
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 3	Ing. Milton Arturo García Lima
Cargo	Jefe de la Unidad de Sistemas para la Evaluación Educativa
Funciones	Realizar el proceso de software (formularios de datos personales para el registro de profesores, alumnos y externos) con la finalidad de atender las necesidades administrativas de la DEE garantizando que la información almacenada es veraz, oportuna y confiable
Obligaciones	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
Nombre de Encargado 4	Lic. Isaac Aboytes Morales
Cargo	Jefe de Departamento de Plataformas de Exámenes
Funciones	Realizar procesos de respaldo y restauración de la información contenida en el sistema
Obligaciones	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad (control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
<b>Usuarios</b>	
<b>Tipo de usuario</b>	<b>Nombre completo</b>
Profesores	Docentes y académicos de la UNAM
Alumnos	Alumnos de la comunidad UNAM



--	--

## 2. ESTRUCTURA Y DESCRIPCIÓN

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-007
Nombre del sistema	Sistema de Análisis Psicométrico de Reactivos (SISAPRE)
Tipo de soporte <sup>25</sup>	Electrónico
Descripción <sup>26</sup>	Base de datos relacional
Características del lugar donde se resguardan los soportes	El centro de datos (versión privada <sup>27</sup> ) es una habitación reservada para los servidores, cuenta con sistema de enfriamiento y redundancia de alimentación eléctrica. El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso. Se cuenta con circuito cerrado que graba los movimientos.

## 3. ANÁLISIS DE RIESGOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-007	
Nombre del sistema	Sistema de Análisis Psicométrico de Reactivos (SISAPRE)	
Riesgo	Impacto	Mitigación
Informático		
Datos de acceso comprometidos	Alto	Renovar claves de acceso
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso
Virus informático	Alto	Instalación de antivirus, Actualización constante del antivirus, Eliminar amenaza en el equipo comprometido, Plan de respaldo y recuperación
Ataque informático	Alto	Identificar y solucionar amenaza(s) y vulnerabilidad(es), Plan de respaldo y recuperación
Pérdida de información	Alto	Plan de respaldo y recuperación
Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos

<sup>25</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

<sup>26</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

<sup>27</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

		Lógico: revisión periódica de servicios y puertos habilitados
		Monitoreo: <ul style="list-style-type: none"> <li>• Sistema de cámaras de circuito cerrado</li> <li>• Sistema de detección de intrusos</li> </ul>
Suministro e instalación eléctrica		
CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado
Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros	Alto	Se cuenta con un plan de respaldo y recuperación de información

#### 4. ANÁLISIS DE BRECHA

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-007	
Nombre del sistema	Sistema de Análisis Psicométrico de Reactivos (SISAPRE)	
Nombre	Causa	Solución
Actualizaciones al sistema operativo	No actualizar el sistema operativo	Actualizaciones periódicas a los sistemas operativos
Actualizaciones la plataforma de desarrollo	Compatibilidad con las versiones de producción. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación
Servidores web y de aplicaciones	Compatibilidad con las versiones de producción de sistemas operativos y librerías. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación
Cuentas de acceso en desuso	Término de relación laboral del personal asignado Falta de notificación al área para realizar la restricción de acceso correspondiente	Revisión periódica de cuentas de usuarios vigentes
Asignación errónea de privilegios de usuario	Equivocación en la creación de cuentas de usuario. Solicitud de cambios en los privilegios en las cuentas de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario
Capacitación a usuarios	Falta de capacitación a usuarios que provoque la falta de confiabilidad en la integridad de la información (nuevos usuarios y/o cambios de rol de usuarios)	Capacitar adecuadamente al personal para los roles asignados
Flujo de la información	Solicitud de omisión de procesos durante el flujo de información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema

## 5. PLAN DE TRABAJO

Dirección de Evaluación Educativa				
Identificador único		CUAIEED-DEE-007		
Nombre del sistema		Sistema de Análisis Psicométrico de Reactivos (SISAPRE)		
Control	Actividades por realizar	Duración	Prioridad	Áreas responsables
Actualizaciones al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones de la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-007
Nombre del sistema	Sistema de Análisis Psicométrico de Reactivos (SISAPRE)
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.

Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital). Filtrado de paquetes desde y hacia el servidor web.
---	--

## II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Sistema de Análisis Psicométrico de Reactivos (SISAPRE) no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

## III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

## IV. REGISTRO DE INCIDENTES

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

## V. ACCESO A LAS INSTALACIONES

*Información reservada*

La vigilancia y el acceso físico al edificio es proporcionado por el personal de los Consejos Académicos de Área. Se cuenta con una caseta de vigilancia que registra todos los accesos para el ingreso a la Dirección de Evaluación Educativa (DEE).

Para el acceso a la DEE cuenta con un lector biométrico de huella digital, el acceso al Centro de Datos está restringido únicamente al personal autorizado de la USEE (cuenta con llave) y además tiene instalado un sistema de circuito cerrado con detección de movimiento.

## VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

## VII. PERFILES DE USUARIO Y CONTRASEÑA

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hackeos* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

## XI. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

*Dirección de Evaluación Educativa*

Identificador único	CUAIEED-DEE-007	
Nombre del sistema	Sistema de Análisis Psicométrico de Reactivos (SISAPRE)	
Recurso	Descripción	Control
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades.  Se realiza un escaneo de puertos de manera periódica con el fin de corroborar que solo estén abiertos los puertos necesarios por la aplicación.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones.
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario autorizado por la DEE (archivo cifrado con protección de contraseña).

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

## 9. MEJORA CONTINUA

*No aplica*

### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-007		
Nombre del sistema	Sistema de Análisis Psicométrico de Reactivos (SISAPRE)		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-007		
Nombre del sistema	Sistema de Análisis Psicométrico de Reactivos (SISAPRE)		
Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-007	
Nombre del sistema	Sistema de Análisis Psicométrico de Reactivos (SISAPRE)	
Proceso	Descripción	Responsable
Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los respaldos automatizados se resguardan de manera indefinida	Unidad de Sistemas para la Evaluación Educativa (USEE)

### 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-007	
Nombre del sistema	Sistema de Análisis Psicométrico de Reactivos (SISAPRE)	
Proceso	Descripción	Responsable
Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)

### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa.

El sistema será eliminado una vez expirado el tiempo solicitado. por medio de requerimiento.

#### Exámenes en Línea (EXAL)

##### Introducción

La plataforma EXAL fue diseñada para permitir la aplicación de exámenes institucionales de ingreso, egreso y diagnóstico a nivel nacional e internacional en aplicaciones presenciales y/o a distancia desde dispositivos de escritorio y móviles. EXAL cuenta únicamente con un perfil de usuario el cual cuenta con privilegios específicos sobre la información generada en el sistema.

#### 1. INVENTARIO

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-008
Nombre del sistema	Exámenes en Línea (EXAL)
Datos personales contenidos en el sistema	<ul style="list-style-type: none"> <li>● Folio de aplicación/número de cuenta</li> <li>● Nombre</li> </ul>

	<ul style="list-style-type: none"> <li>● Apellido Paterno</li> <li>● Apellido Materno **</li> <li>● Fecha de nacimiento</li> <li>● Género</li> <li>● Subsistema **</li> <li>● Área **</li> <li>● Plantel **</li> </ul>
<b>** Información opcional</b>	
<b>Responsable:</b>	<b>Dirección de Evaluación Educativa</b>
Nombre:	Dr. Adrián Martínez
Cargo:	Director de Evaluación Educativa
Funciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones:	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>Encargados</b>	
Nombre de Encargado 2	Mtra. Nancy Sofía Contreras Michel
Cargo	Subdirectora de Evaluación de Posgrado y Titulación
Funciones	Brindar seguimiento a los procesos de registro de usuarios (sustentantes)
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 2	Lic. Enrique Ricardo Buzo Casanova
Cargo	Subdirector de Evaluación de Bachillerato y Licenciatura
Funciones	Brindar seguimiento a los procesos de registro de usuarios (sustentantes)
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 3	Ing. Milton Arturo García Lima
Cargo	Jefe de la Unidad de Sistemas para la Evaluación Educativa
Funciones	Realizar el proceso de software (formularios de datos personales para el registro de sustentantes con la finalidad de atender las necesidades administrativas de la DEE garantizando que la información almacenada es veraz, oportuna y confiable
Obligaciones	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
Nombre de Encargado 4	Lic. Isaac Aboytes Morales
Cargo	Jefe de Departamento de Plataformas de Exámenes
Funciones	Realizar procesos de respaldo y restauración de la información contenida en el sistema
Obligaciones	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad (control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
<b>Usuarios</b>	
<b>Tipo de usuario</b>	<b>Nombre completo</b>
Profesores	Docentes y académicos de la UNAM
Sustentantes	Población en general y de la comunidad UNAM

## 2. ESTRUCTURA Y DESCRIPCIÓN

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-008
Nombre del sistema	Exámenes en Línea (EXAL)
Tipo de soporte <sup>28</sup>	Electrónico
Descripción <sup>29</sup>	Base de datos relacional
Características del lugar donde se resguardan los soportes	El centro de datos (versión privada <sup>30</sup> ) es una habitación reservada para los servidores, cuenta con sistema de enfriamiento y redundancia de alimentación eléctrica. El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso. Se cuenta con circuito cerrado que graba los movimientos

## 3. ANÁLISIS DE RIESGOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-008	
Nombre del sistema	Exámenes en Línea (EXAL)	
Riesgo	Impacto	Mitigación
Informático		
Datos de acceso comprometidos	Alto	Renovar claves de acceso
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso
Virus informático	Alto	Instalación de antivirus Actualización constante del antivirus Eliminar amenaza en el equipo comprometido Plan de respaldo y recuperación
Ataque informático	Alto	Identificar y solucionar amenaza(s) y vulnerabilidad(es) Plan de respaldo y recuperación
Pérdida de información	Alto	Plan de respaldo y recuperación
Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos

<sup>28</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

<sup>29</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

<sup>30</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.



		Lógico: revisión periódica de servicios y puertos habilitados
		Monitoreo: <ul style="list-style-type: none"> <li>• Sistema de cámaras de circuito cerrado</li> <li>• Sistema de detección de intrusos</li> </ul>
Suministro e instalación eléctrica		
CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado
Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros	Alto	Se cuenta con un plan de respaldo y recuperación de información

#### 4. ANÁLISIS DE BRECHA

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-008	
Nombre del sistema	Exámenes en Línea (EXAL)	
Nombre	Causa	Solución
Actualizaciones al sistema operativo	No actualizar el sistema operativo	Actualizaciones periódicas a los sistemas operativos
Actualizaciones la plataforma de desarrollo	Compatibilidad con las versiones de producción. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación
Servidores web y de aplicaciones	Compatibilidad con las versiones de producción de sistemas operativos y librerías. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación
Cuentas de acceso en desuso	Término de relación laboral del personal asignado Falta de notificación al área para realizar la restricción de acceso correspondiente	Revisión periódica de cuentas de usuarios vigentes
Asignación errónea de privilegios de usuario	Equivocación en la creación de cuentas de usuario. Solicitud de cambios en los privilegios en las cuentas de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario
Capacitación a usuarios	Falta de capacitación a usuarios que provoque la falta de confiabilidad en la integridad de la información (nuevos usuarios y/o cambios de rol de usuarios)	Capacitar adecuadamente al personal para los roles asignados
Flujo de la información	Solicitud de omisión de procesos durante el flujo de información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema

## 5. PLAN DE TRABAJO

Dirección de Evaluación Educativa				
Identificador único		CUAIEED-DEE-008		
Nombre del sistema		Exámenes en Línea (EXAL)		
Control	Actividades por realizar	Duración	Prioridad	Áreas responsables
Actualizaciones al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-008
Nombre del sistema	Exámenes en Línea (EXAL)
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital). Filtrado de paquetes desde y hacia el servidor web.

### II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El sistema de Exámenes en Línea (EXAL) no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

### III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

### IV. REGISTRO DE INCIDENTES

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

### V. ACCESO A LAS INSTALACIONES

La vigilancia y el acceso físico al edificio es proporcionado por el personal de los Consejos Académicos de Área. Se cuenta con una caseta de vigilancia que registra todos los accesos para el ingreso a la Dirección de Evaluación Educativa (DEE).  
Para el acceso a la DEE cuenta con un lector biométrico de huella digital, el acceso al Centro de Datos está restringido únicamente al personal autorizado de la USEE (cuenta con llave) y además tiene instalado un sistema de circuito cerrado con detección de movimiento.

### VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

### VII. PERFILES DE USUARIO Y CONTRASEÑA

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hacks* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

### VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

### XI. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

### 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-008	
Nombre del sistema	Exámenes en Línea (EXAL)	
Recurso	Descripción	Control
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades. Se realiza un escaneo de puertos de manera periódica con el fin de corroborar

		que solo estén abiertos los puertos necesarios por la aplicación.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones.
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario autorizado por la DEE (archivo cifrado con protección de contraseña).

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

## 9. MEJORA CONTINUA

*No aplica*

### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-008		
Nombre del sistema	Exámenes en Línea (EXAL)		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-008		
Nombre del sistema	Exámenes en Línea (EXAL)		
Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-008	
Nombre del sistema	Exámenes en Línea (EXAL)	
Proceso	Descripción	Responsable
Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los respaldos automatizados se resguardan de manera indefinida	Unidad de Sistemas para la Evaluación Educativa (USEE)

## 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-008	
Nombre del sistema	Exámenes en Línea (EXAL)	
Proceso	Descripción	Responsable
Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa. El sistema será eliminado una vez expirado el tiempo solicitado. por medio de requerimiento.

### Sistema de Planes y Programas de Estudio (SIPPE)

#### Introducción

El Sistema de Planes y Programas de Estudio (SIPPE) permite la correcta gestión de los procesos de propuesta (anteproyecto), elaboración, revisión, aprobación, modificación, evaluación y consulta de Planes y Programas de estudio de la Universidad Nacional Autónoma de México. El SIPPE cuenta con cuatro roles de usuario y cada uno de ellos posee privilegios específicos sobre la información alojada en el sistema. 1) Entidad: Proporciona toda la información del anteproyecto, puede guardar el avance incremental y generar una vista previa de cada módulo en el que se encuentre trabajando. Cada módulo cuenta con criterios los cuales se deben de cumplir para continuar con el proceso. En todo momento puede ver el porcentaje de avance. 2) Revisor: Usuario de la Subdirección de Planes y Programas de Estudio (SPPE), encargado de realizar la etapa de primera revisión y validación de la información enviada por la entidad. 3) Coordinador: Usuario de la SPPE encargado de realizar la segunda etapa de revisión/aprobación de la información que conforma el Anteproyecto. 4) Administrador del sistema: responsable de la gestión de usuarios, anteproyectos, catálogos base y creación de grupos de trabajo. Soporte al sistema y usuarios.

#### 1. INVENTARIO

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único	CUAIEED-DEE-009
Nombre del sistema	Sistema de Planes y Programas de Estudio (SIPPE)
Datos personales contenidos en el sistema Entidad	Información proporcionada mediante un oficio
Revisor	Información proporcionada mediante un oficio
Coordinador	Información proporcionada mediante un oficio
Administrador del sistema	Información proporcionada mediante un oficio

<b>Responsable:</b>	<b>Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente</b>
Nombre:	Mtra. María del Pilar Martínez Hernández
Cargo:	Directora de Innovación Educativa, Desarrollo Curricular y Formación Docente
Funciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones:	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>Encargados</b>	
Nombre de Encargado 2	Mtra. Cecilia Montiel Ayometzi
Cargo	Subdirectora de Planes y Programas de Estudio
Funciones	Brindar seguimiento a los procesos de registro de usuarios (entidad, revisor y coordinador)
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 3	Ing. Milton Arturo García Lima
Cargo	Jefe de la Unidad de Sistemas para la Evaluación Educativa
Funciones	Realizar el proceso de software (formularios de datos personales para el registro los responsables de entidad, revisores y coordinadores) con la finalidad de atender las necesidades administrativas de la DEE garantizando que la información almacenada es veraz, oportuna y confiable
Obligaciones	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
Nombre de Encargado 4	Lic. Isaac Aboytes Morales
Cargo	Jefe de Departamento de Plataformas de Exámenes
Funciones	Realizar procesos de respaldo y restauración de la información contenida en el sistema
Obligaciones	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad (control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
<b>Usuarios</b>	
<i>Usuarios</i>	
<b>Tipo de usuario</b>	<b>Nombre completo</b>
Entidad	Docentes y académicos de la UNAM
Revisor	Docentes y académicos de la UNAM
Coordinador	Docentes y académicos de la UNAM
Administrador del sistema	Personal autorizado CUAIEED

## 2. ESTRUCTURA Y DESCRIPCIÓN

<b>Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente</b>	
Identificador único	CUAIEED-DEE-009
Nombre del sistema	Sistema de Planes y Programas de Estudio (SIPPE)

Tipo de soporte <sup>31</sup>	Electrónico
Descripción <sup>32</sup>	Base de datos relacional
Características del lugar donde se resguardan los soportes	El centro de datos (versión privada <sup>33</sup> ) es una habitación reservada para los servidores, cuenta con sistema de enfriamiento y redundancia de alimentación eléctrica. El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso. Se cuenta con circuito cerrado que graba los movimientos

### 3. ANÁLISIS DE RIESGOS

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único	CUAIEED-DEE-009	
Nombre del sistema	Sistema de Planes y Programas de Estudio (SIPPE)	
Riesgo	Impacto	Mitigación
Informático		
Datos de acceso comprometidos	Alto	Renovar claves de acceso
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso
Virus informático	Alto	Instalación de antivirus. Actualización constante del antivirus. Eliminar amenaza en el equipo comprometido.
Ataque informático	Alto	Plan de respaldo y recuperación. Identificar y solucionar amenaza(s) y vulnerabilidad(es). Plan de respaldo y recuperación.
Pérdida de información	Alto	Plan de respaldo y recuperación.
Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos.  Lógico: revisión periódica de servicios y puertos habilitados.  Monitoreo: <ul style="list-style-type: none"> <li>• Sistema de cámaras de circuito cerrado</li> <li>• Sistema de detección de intrusos</li> </ul>

<sup>31</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

<sup>32</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

<sup>33</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

Suministro e instalación eléctrica		
CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado
Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros	Alto	Se cuenta con un plan de respaldo y recuperación de información

#### 4. ANÁLISIS DE BRECHA

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único	CUAIEED-DEE-009	
Nombre del sistema	Sistema de Planes y Programas de Estudio (SIPPE)	
Nombre	Causa	Solución
Actualizaciones al sistema operativo	No actualizar el sistema operativo	Actualizaciones periódicas a los sistemas operativos
Actualizaciones la plataforma de desarrollo	Compatibilidad con las versiones de producción. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación
Servidores web y de aplicaciones	Compatibilidad con las versiones de producción de sistemas operativos y librerías. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación
Cuentas de acceso en desuso	Término de relación laboral del personal asignado. Falta de notificación al área para realizar la restricción de acceso correspondiente	Revisión periódica de cuentas de usuarios vigentes
Asignación errónea de privilegios de usuario	Equivocación en la creación de cuentas de usuario. Solicitud de cambios en los privilegios en las cuentas de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario
Capacitación a usuarios	Falta de capacitación a usuarios que provoque la falta de confiabilidad en la integridad de la información (nuevos usuarios y/o cambios de rol de usuarios)	Capacitar adecuadamente al personal para los roles asignados
Flujo de la información	Solicitud de omisión de procesos durante el flujo de información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema

#### 5. PLAN DE TRABAJO

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único	CUAIEED-DEE-009
Nombre del sistema	Sistema de Planes y Programas de Estudio (SIPPE)



Control	Actividades por realizar	Duración	Prioridad	Áreas responsables
Actualizaciones al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones de la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único	CUAIEED-DEE-009
Nombre del sistema	Sistema de Planes y Programas de Estudio (SIPPE)
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital). Filtrado de paquetes desde y hacia el servidor web.

## II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Sistema de Planes y Programas de Estudio (SIPPE) no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

## III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

## IV. REGISTRO DE INCIDENTES

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

## V. ACCESO A LAS INSTALACIONES

La vigilancia y el acceso físico al edificio es proporcionado por el personal de los Consejos Académicos de Área. Se cuenta con una caseta de vigilancia que registra todos los accesos para el ingreso a la Dirección de Evaluación Educativa (DEE). Para el acceso a la DEE cuenta con un lector biométrico de huella digital, el acceso al Centro de Datos está restringido únicamente al personal autorizado de la USEE (cuenta con llave) y además tiene instalado un sistema de circuito cerrado con detección de movimiento.

## VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

## VII. PERFILES DE USUARIO Y CONTRASEÑA

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hackeos* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

## XI. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único	QUAIEED-DEE-009	
Nombre del sistema	Sistema de Planes y Programas de Estudio (SIPPE)	
Recurso	Descripción	Control
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades.

	escaneo de puertos abiertos	Se realiza un escaneo de puertos de manera periódica con el fin de corroborar que solo estén abiertos los puertos necesarios por la aplicación
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario autorizado por la DEE (archivo cifrado con protección de contraseña)

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

## 9. MEJORA CONTINUA

*No aplica*

### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente			
Identificador único	CUAIEED-DEE-009		
Nombre del sistema	Sistema de Planes y Programas de Estudio (SIPPE)		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente			
Identificador único	CUAIEED-DEE-009		
Nombre del sistema	Sistema de Planes y Programas de Estudio (SIPPE)		
Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único	CUAIEED-DEE-009	
Nombre del sistema	Sistema de Planes y Programas de Estudio (SIPPE)	
Proceso	Descripción	Responsable
Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los respaldos	Unidad de Sistemas para la Evaluación Educativa (USEE)

	automatizados se resguardan de manera indefinida	
--	--	--

#### 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único	CUAIEED-DEE-009	
Nombre del sistema	Sistema de Planes y Programas de Estudio (SIPPE)	
Proceso	Descripción	Responsable
Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)

#### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa. El sistema será eliminado una vez expirado el tiempo solicitado. por medio de requerimiento.

#### Sistema de Evaluación de la Docencia y la Tutoría

##### Introducción

El Sistema de Evaluación de la Docencia y la Tutoría tiene el propósito de valorar, de manera justa y situada, el desempeño del personal académico. El sistema de Evaluación cuenta con dos roles de usuario y cada uno de ellos posee privilegios específicos sobre la información alojada en el sistema. 1) responsable de entidad: Proporciona toda la información del personal académico, asignaciones y la matrícula de estudiantes para la evaluación en turno. 2) Alumno: es el responsable de responder los cuestionarios que le son asignados durante la evaluación docente, al finalizar podrá generar un archivo que servirá como comprobante para futuros trámites en su institución académica.

##### 1. INVENTARIO

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-010
Nombre del sistema	Sistema de Evaluación de la Docencia y la Tutoría
Datos personales contenidos en el sistema	<ul style="list-style-type: none"> <li>● Nombre</li> <li>● Apellido paterno</li> <li>● Apellido materno</li> <li>● Correo electrónico</li> </ul>
<ul style="list-style-type: none"> <li>● Alumno *</li> </ul>	<ul style="list-style-type: none"> <li>● Número de cuenta</li> <li>● Nombre</li> <li>● Apellido paterno</li> <li>● Apellido materno</li> <li>● Fecha de nacimiento</li> <li>● Género</li> </ul>

	• Edad
<i>* Información proporcionada por el responsable de entidad</i>	
<b>Responsable:</b>	<b>Dirección de Evaluación Educativa</b>
Nombre:	Dr. Adrián Martínez
Cargo:	Director de Evaluación Educativa
Funciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones:	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>Encargados</b>	
Nombre de Encargado 2	Mtra. Laura Elena Rojo Chávez
Cargo	Subdirectora de Evaluación de Procesos y Programas Académicos
Funciones	Brindar seguimiento a los procesos de registro de usuarios (responsables de entidad, responsables de programa, docentes, tutores y alumnos)
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 3	Ing. Milton Arturo García Lima
Cargo	Jefe de la Unidad de Sistemas para la Evaluación Educativa
Funciones	Realizar el proceso de software (formularios de datos personales para el registro los responsables de entidad, responsables de programa, docentes, tutores y alumnos) con la finalidad de atender las necesidades administrativas de la DEE garantizando que la información almacenada es veraz, oportuna y confiable
Obligaciones	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
Nombre de Encargado 4	Lic. Isaac Aboytes Morales
Cargo	Jefe de Departamento de Plataformas de Exámenes
Funciones	Realizar procesos de respaldo y restauración de la información contenida en el sistema
Obligaciones	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad (control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
<b>Usuarios</b>	
<b>Tipo de usuario</b>	<b>Nombre completo</b>
Responsables de entidad	Académicos de la UNAM
Alumnos	Alumnos de la comunidad UNAM

## 2. ESTRUCTURA Y DESCRIPCIÓN

<b>Dirección de Evaluación Educativa</b>	
Identificador único	CUAIEED-DEE-010
Nombre del sistema	Sistema de Evaluación de la Docencia y la Tutoría

Tipo de soporte <sup>34</sup>	Electrónico
Descripción <sup>35</sup>	Base de datos relacional
Características del lugar donde se resguardan los soportes	El centro de datos (versión privada <sup>36</sup> ) es una habitación reservada para los servidores, cuenta con sistema de enfriamiento y redundancia de alimentación eléctrica. El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso. Se cuenta con circuito cerrado que graba los movimientos

### 3. ANÁLISIS DE RIESGOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-010	
Nombre del sistema	Sistema de Evaluación de la Docencia y la Tutoría	
Riesgo	Impacto	Mitigación
Informático		
Datos de acceso comprometidos	Alto	Renovar claves de acceso
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso
Virus informático	Alto	Instalación de antivirus. Actualización constante del antivirus. Eliminar amenaza en el equipo comprometido. Plan de respaldo y recuperación.
Ataque informático	Alto	Identificar y solucionar amenaza(s) y vulnerabilidad(es). Plan de respaldo y recuperación.
Pérdida de información	Alto	Plan de respaldo y recuperación.
Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos.  Lógico: revisión periódica de servicios y puertos habilitados.  Monitoreo: <ul style="list-style-type: none"> <li>• Sistema de cámaras de circuito cerrado</li> <li>• Sistema de detección de intrusos</li> </ul>

<sup>34</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

<sup>35</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

<sup>36</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

Suministro e instalación eléctrica		
CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado
Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros	Alto	Se cuenta con un plan de respaldo y recuperación de información

#### 4. ANÁLISIS DE BRECHA

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-010	
Nombre del sistema	Sistema de Evaluación de la Docencia y la Tutoría	
Nombre	Causa	Solución
Actualizaciones al sistema operativo	No actualizar el sistema operativo	Actualizaciones periódicas a los sistemas operativos
Actualizaciones la plataforma de desarrollo	Compatibilidad con las versiones de producción. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación
Servidores web y de aplicaciones	Compatibilidad con las versiones de producción de sistemas operativos y librerías. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación
Cuentas de acceso en desuso	Término de relación laboral del personal asignado. Falta de notificación al área para realizar la restricción de acceso correspondiente	Revisión periódica de cuentas de usuarios vigentes
Asignación errónea de privilegios de usuario	Equivocación en la creación de cuentas de usuario. Solicitud de cambios en los privilegios en las cuentas de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario
Capacitación a usuarios	Falta de capacitación a usuarios que provoque la falta de confiabilidad en la integridad de la información (nuevos usuarios y/o cambios de rol de usuarios)	Capacitar adecuadamente al personal para los roles asignados
Flujo de la información	Solicitud de omisión de procesos durante el flujo de información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema

#### 5. PLAN DE TRABAJO

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-010	

Nombre del sistema	Actividades por realizar	Duración	Prioridad	Áreas responsables
Control al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones de la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-010
Nombre del sistema	Sistema de Evaluación de la Docencia y la Tutoría
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital). Filtrado de paquetes desde y hacia el servidor web.



## II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Sistema de Evaluación de la Docencia y la Tutoría genera informe(s) que contiene(n) datos personales del usuario (alumnos) mismos que son resguardados por el usuario responsable de la cuenta.

## III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

## IV. REGISTRO DE INCIDENTES

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

## V. ACCESO A LAS INSTALACIONES

Información reservada

La vigilancia y el acceso físico al edificio es proporcionado por el personal de los Consejos Académicos de Área. Se cuenta con una caseta de vigilancia que registra todos los accesos para el ingreso a la Dirección de Evaluación Educativa (DEE).

Para el acceso a la DEE cuenta con un lector biométrico de huella digital, el acceso al Centro de Datos está restringido únicamente al personal autorizado de la USEE (cuenta con llave) y además tiene instalado un sistema de circuito cerrado con detección de movimiento.

## VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

## VII. PERFILES DE USUARIO Y CONTRASEÑA

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hacks* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

## XI. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Dirección de Evaluación Educativa		
Identificador único	QUAIEED-DEE-010	
Nombre del sistema	Sistema de Evaluación de la Docencia y la Tutoría	
Recurso	Descripción	Control

Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades.  Se realiza un escaneo de puertos de manera periódica con el fin de corroborar que solo estén abiertos los puertos necesarios por la aplicación.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones.
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales.	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario autorizado por la DEE (archivo cifrado con protección de contraseña).

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

## 9. MEJORA CONTINUA

*No aplica*

### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-010		
Nombre del sistema	Sistema de Evaluación de la Docencia y la Tutoría		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-010		
Nombre del sistema	Sistema de Evaluación de la Docencia y la Tutoría		
Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-010	
Nombre del sistema	Sistema de Evaluación de la Docencia y la Tutoría	
Proceso	Descripción	Responsable

Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los respaldos automatizados se resguardan de manera indefinida	Unidad de Sistemas para la Evaluación Educativa (USEE)
---	---	--

#### 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-010	
Nombre del sistema	Sistema de Evaluación de la Docencia y la Tutoría	
Proceso	Descripción	Responsable
Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)

#### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa. El sistema será eliminado una vez expirado el tiempo solicitado. por medio de requerimiento.

#### Sistema de Gestión de Concursos

##### Introducción

El Sistema de Gestión de Concursos tiene el propósito de recabar los trabajos que cumplan con los criterios de calidad establecidos, para ser sujeto a una serie de evaluaciones por expertos en la materia (según los fines de la convocatoria) y además de seleccionar los trabajos sobresalientes, permite conocer las diversas opiniones de todos los participantes. El Sistema de Gestión de Concursos cuenta con tres roles de usuario y cada uno de ellos posee privilegios específicos sobre la información alojada en el sistema. 1) Administrador del sistema: cuenta con los privilegios necesarios para monitorear en todo momento el desarrollo del concurso (conocer el estatus de cada trabajo), obtener información de los registros de participantes y trabajos en la plataforma. 2) Comité técnico/académico: realiza las revisiones de los trabajos participantes de acuerdo con los criterios de evaluación. 3) Participante: proporciona la información de datos personales solicitada por el sistema y puede realizar el registro de trabajos en la plataforma.

#### 1. INVENTARIO

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único	CUAIEED-DEE-011
Nombre del sistema	Sistema de Gestión de Concursos
Datos personales contenidos en el sistema <ul style="list-style-type: none"> <li>Administrador</li> </ul>	<ul style="list-style-type: none"> <li>Nombre</li> <li>Apellido paterno</li> <li>Apellido materno</li> <li>Correo electrónico</li> </ul>
<ul style="list-style-type: none"> <li>Comité técnico</li> <li>Comité académico</li> </ul>	<i>Información proporcionada por el responsable del concurso</i> <ul style="list-style-type: none"> <li>Nombre</li> <li>Apellido paterno</li> <li>Apellido materno</li> </ul>

	<ul style="list-style-type: none"> <li>● Correo electrónico</li> </ul>
<ul style="list-style-type: none"> <li>● Participantes<sup>37</sup></li> </ul>	<ul style="list-style-type: none"> <li>● Nombre</li> <li>● Apellido paterno</li> <li>● Apellido materno</li> <li>● Fecha de nacimiento</li> <li>● Correo electrónico</li> <li>● Número de trabajador</li> <li>● RFC</li> <li>● Planteles de adscripción</li> </ul>
<b>Responsable:</b>	<b>Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente</b>
Nombre:	Mtra. María del Pilar Martínez Hernández
Cargo:	Directora de Innovación Educativa, Desarrollo Curricular y Formación Docente
Funciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones:	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>Encargados</b>	
Nombre de Encargado 2	Mtra. Cecilia Montiel Ayometzi
Cargo	Subdirectora de Planes y Programas de Estudio
Funciones	Brindar seguimiento a los procesos de registro de usuarios (comité técnico, comité académico, participantes)
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 3	Ing. Milton Arturo García Lima
Cargo	Jefe de la Unidad de Sistemas para la Evaluación Educativa
Funciones	Realizar el proceso de software (formularios de datos personales para el registro de miembros del comité técnico, comité tutor y participantes) con la finalidad de atender las necesidades administrativas de la DEIC garantizando que la información almacenada es veraz, oportuna y confiable
Obligaciones	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
Nombre de Encargado 4	Lic. Isaac Aboytes Morales
Cargo	Jefe de Departamento de Plataformas de Exámenes
Funciones	Realizar procesos de respaldo y restauración de la información contenida en el sistema
Obligaciones	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad (control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
<b>Usuarios</b>	
<b>Tipo de usuario</b>	<b>Nombre completo</b>
Administrador	Personal autorizado CUAIEED
Comité técnico y comité académico	Docentes y académicos de la UNAM
Participantes	Docentes y académicos de la UNAM

<sup>37</sup> Los datos personales de los participantes que recaba el sistema dependen de la convocatoria, ya que cada concurso va dirigido a diferente población y, por ende, el tipo de información solicitada. En el último concurso "Colección de testimonios PEG" iba dirigido a académicos y docentes de la UNAM.

## 2. ESTRUCTURA Y DESCRIPCIÓN

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único	CUAIEED-DEE-011
Nombre del sistema	Sistema de Gestión de Concursos
Tipo de soporte <sup>38</sup>	Electrónico
Descripción <sup>39</sup>	Base de datos relacional
Características del lugar donde se resguardan los soportes	El centro de datos (versión privada <sup>40</sup> ) es una habitación reservada para los servidores, cuenta con sistema de enfriamiento y redundancia de alimentación eléctrica. El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso. Se cuenta con circuito cerrado que graba los movimientos

## 3. ANÁLISIS DE RIESGOS

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único	CUAIEED-DEE-011	
Nombre del sistema	Sistema de Gestión de Concursos	
Riesgo	Impacto	Mitigación
Informático		
Datos de acceso comprometidos	Alto	Renovar claves de acceso
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso
Virus informático	Alto	Instalación de antivirus. Actualización constante del antivirus. Eliminar amenaza en el equipo comprometido. Plan de respaldo y recuperación.
Ataque informático	Alto	Identificar y solucionar amenaza(s) y vulnerabilidad(es). Plan de respaldo y recuperación.
Pérdida de información	Alto	Plan de respaldo y recuperación.
Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos

<sup>38</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

<sup>39</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

<sup>40</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

		Lógico: revisión periódica de servicios y puertos habilitados
		Monitoreo: <ul style="list-style-type: none"> <li>Sistema de cámaras de circuito cerrado</li> <li>Sistema de detección de intrusos</li> </ul>
Suministro e instalación eléctrica		
CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado
Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros	Alto	Se cuenta con un plan de respaldo y recuperación de información

#### 4. ANÁLISIS DE BRECHA

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único	CUAIEED-DEE-011	
Nombre del sistema	Sistema de Gestión de Concursos	
Nombre	Causa	Solución
Actualizaciones al sistema operativo	No actualizar el sistema operativo	Actualizaciones periódicas a los sistemas operativos
Actualizaciones la plataforma de desarrollo	Compatibilidad con las versiones de producción. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación
Servidores web y de aplicaciones	Compatibilidad con las versiones de producción de sistemas operativos y librerías. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación
Cuentas de acceso en desuso	Término de relación laboral del personal asignado Falta de notificación al área para realizar la restricción de acceso correspondiente	Revisión periódica de cuentas de usuarios vigentes
Asignación errónea de privilegios de usuario	Equivocación en la creación de cuentas de usuario. Solicitud de cambios en los privilegios en las cuentas de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario
Capacitación a usuarios	Falta de capacitación a usuarios que provoque la falta de confiabilidad en la integridad de la información (nuevos usuarios y/o cambios de rol de usuarios)	Capacitar adecuadamente al personal para los roles asignados
Flujo de la información	Solicitud de omisión de procesos durante el flujo de información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema

## 5. PLAN DE TRABAJO

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente				
Identificador único	CUAIEED-DEE-011			
Nombre del sistema	Sistema de Gestión de Concursos			
Control	Actividades por realizar	Duración	Prioridad	Áreas responsables
Actualizaciones al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones de la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único	CUAIEED-DEE-011
Nombre del sistema	Sistema de Gestión de Concursos
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital).

## II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Sistema de Gestión de Concursos no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

## III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

## IV. REGISTRO DE INCIDENTES

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

## V. ACCESO A LAS INSTALACIONES



## VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

## VII. PERFILES DE USUARIO Y CONTRASEÑA

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hacks* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

## XI. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente

Identificador único	QUAIEED-DEE-01	
Nombre del sistema	Sistema de Gestión de Concursos	
Recurso	Descripción	Control



Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades.  Se realiza un escaneo de puertos de manera periódica con el fin de corroborar que solo estén abiertos los puertos necesarios por la aplicación.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones.
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales.	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario autorizado por la DEE (archivo cifrado con protección de contraseña).

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

## 9. MEJORA CONTINUA

*No aplica*

### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente			
Identificador único	CUAIEED-DEE-011		
Nombre del sistema	Sistema de Gestión de Concursos		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente			
Identificador único	CUAIEED-DEE-011		
Nombre del sistema	Sistema de Gestión de Concursos		
Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único	CUAIEED-DEE-011
Nombre del sistema	Sistema de Gestión de Concursos

Proceso	Descripción	Responsable
Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los respaldos automatizados se resguardan de manera indefinida	Unidad de Sistemas para la Evaluación Educativa (USEE)

#### 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único	CUAIEED-DEE-011	
Nombre del sistema	Sistema de Gestión de Concursos	
Proceso	Descripción	Responsable
Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)

#### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa. El sistema será eliminado una vez expirado el tiempo solicitado. por medio de requerimiento.

#### Plataforma Moodle. Comisión Especial de Lenguas

##### Introducción

Entorno digital o aula virtual dedicada al desarrollo de un proceso de evaluación para la Comisión Especial de Lenguas.

##### 1. INVENTARIO

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-012
Nombre del sistema	Plataforma Moodle. Comisión Especial de Lenguas
Datos personales contenidos en el sistema <sup>41</sup>	<ul style="list-style-type: none"> <li>● Nombre</li> <li>● Apellido paterno</li> <li>● Apellido materno</li> <li>● Correo electrónico</li> </ul>
<ul style="list-style-type: none"> <li>● Alumnos</li> </ul>	<i>Información proporcionada por el responsable del concurso</i> <ul style="list-style-type: none"> <li>● Nombre</li> <li>● Apellido paterno</li> <li>● Apellido materno</li> <li>● Correo electrónico</li> </ul>

<sup>41</sup> Los datos personales son proporcionados por el coordinador del programa de la Comisión Especial de Lenguas

<b>Responsable:</b>	<b>Dirección de Evaluación Educativa</b>
Nombre:	Dr. Adrián Martínez
Cargo:	Director de Evaluación Educativa
Funciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones:	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>Nombre de Encargado 2</b>	<b>Lic. Enrique Ricardo Buzo Casanova</b>
Cargo	Subdirector de Evaluación de Bachillerato y Licenciatura
Funciones	Brindar seguimiento a los procesos de registro de usuarios (profesores y alumnos)
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
<b>Nombre de Encargado 3</b>	<b>Ing. Milton Arturo García Lima</b>
Cargo	Jefe de la Unidad de Sistemas para la Evaluación Educativa
Funciones	Realizar el proceso de software (formularios de datos personales para el registro de profesores y alumnos) con la finalidad de atender las necesidades administrativas de la DEE garantizando que la información almacenada es veraz, oportuna y confiable
Obligaciones	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
<b>Nombre de Encargado 4</b>	<b>Lic. Isaac Aboytes Morales</b>
Cargo	Jefe de Departamento de Plataformas de Exámenes
Funciones	Realizar procesos de respaldo y restauración de la información contenida en el sistema
Obligaciones	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad (control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
<b>Usuarios</b>	
<b>Tipo de usuario</b>	<b>Nombre completo</b>
Profesores	Docentes y académicos de la UNAM
Alumnos	Alumnos de la comunidad UNAM

## 2. ESTRUCTURA Y DESCRIPCIÓN

<b>Dirección de Evaluación Educativa</b>	
Identificador único	CUAIEED-DEE-012
Nombre del sistema	Plataforma Moodle. Comisión Especial de Lenguas
Tipo de soporte <sup>42</sup>	Electrónico

<sup>42</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

Descripción <sup>43</sup>	Base de datos relacional
Características del lugar donde se resguardan los soportes	El centro de datos (versión privada <sup>44</sup> ) es una habitación reservada para los servidores, cuenta con sistema de enfriamiento y redundancia de alimentación eléctrica. El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso. Se cuenta con circuito cerrado que graba los movimientos

### 3. ANÁLISIS DE RIESGOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-012	
Nombre del sistema	Plataforma Moodle Comisión Especial de Lenguas	
Riesgo	Impacto	Mitigación
Informático		
Datos de acceso comprometidos	Alto	Renovar claves de acceso
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso
Virus informático	Alto	Instalación de antivirus. Actualización constante del antivirus. Eliminar amenaza en el equipo comprometido. Plan de respaldo y recuperación
Ataque informático	Alto	Identificar y solucionar amenaza(s) y vulnerabilidad(es). Plan de respaldo y recuperación
Pérdida de información	Alto	Plan de respaldo y recuperación
Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos  Lógico: revisión periódica de servicios y puertos habilitados  Monitoreo: <ul style="list-style-type: none"> <li>• Sistema de cámaras de circuito cerrado</li> <li>• Sistema de detección de intrusos</li> </ul>
Suministro e instalación eléctrica		

<sup>43</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

<sup>44</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado
Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros	Alto	Se cuenta con un plan de respaldo y recuperación de información

#### 4. ANÁLISIS DE BRECHA

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-012	
Nombre del sistema	Plataforma Moodle Comisión Especial de Lenguas	
Nombre	Causa	Solución
Actualizaciones al sistema operativo	No actualizar el sistema operativo	Actualizaciones periódicas a los sistemas operativos
Actualizaciones la plataforma de desarrollo	Compatibilidad con las versiones de producción. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación
Servidores web y de aplicaciones	Compatibilidad con las versiones de producción de sistemas operativos y librerías. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación
Cuentas de acceso en desuso	Término de relación laboral del personal asignado. Falta de notificación al área para realizar la restricción de acceso correspondiente	Revisión periódica de cuentas de usuarios vigentes
Asignación errónea de privilegios de usuario	Equivocación en la creación de cuentas de usuario. Solicitud de cambios en los privilegios en las cuentas de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario
Capacitación a usuarios	Falta de capacitación a usuarios que provoque la falta de confiabilidad en la integridad de la información (nuevos usuarios y/o cambios de rol de usuarios)	Capacitar adecuadamente al personal para los roles asignados
Flujo de la información	Solicitud de omisión de procesos durante el flujo de información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema

#### 5. PLAN DE TRABAJO

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-012
Nombre del sistema	Plataforma Moodle

		Comisión Especial de Lenguas		
Control	Actividades por realizar	Duración	Prioridad	Áreas responsables
Actualizaciones al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones de la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-012
Nombre del sistema	Plataforma Moodle. Comisión Especial de Lenguas
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital). Filtrado de paquetes desde y hacia el servidor web.

### II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS

La Plataforma Moodle no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

### III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

### IV. REGISTRO DE INCIDENTES

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

### V. ACCESO A LAS INSTALACIONES

La vigilancia y el acceso físico al edificio es proporcionado por el personal de los Consejos Académicos de Área. Se cuenta con una caseta de vigilancia que registra todos los accesos para el ingreso a la Dirección de Evaluación Educativa (DEE).  
Para el acceso a la DEE cuenta con un lector biométrico de huella digital, el acceso al Centro de Datos está restringido únicamente al personal autorizado de la USEE (cuenta con llave) y además tiene instalado un sistema de circuito cerrado con detección de movimiento.

### VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

### VII. PERFILES DE USUARIO Y CONTRASEÑA

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hacks* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

### VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

### XI. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

### 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-012	
Nombre del sistema	Plataforma Moodle Comisión Especial de Lenguas	
Recurso	Descripción	Control
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades.

		Se realiza un escaneo de puertos de manera periódica con el fin de corroborar que solo estén abiertos los puertos necesarios por la aplicación.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones.
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario autorizado por la DEE (archivo cifrado con protección de contraseña).

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

## 9. MEJORA CONTINUA

*No aplica.*

### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-012		
Nombre del sistema	Plataforma Moodle. Comisión Especial de Lenguas		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-012		
Nombre del sistema	Plataforma Moodle. Comisión Especial de Lenguas		
Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-012	
Nombre del sistema	Plataforma Moodle. Comisión Especial de Lenguas	
Proceso	Descripción	Responsable



Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los respaldos automatizados se resguardan de manera indefinida	Unidad de Sistemas para la Evaluación Educativa (USEE)
---	---	--

#### 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-012	
Nombre del sistema	Plataforma Moodle. Comisión Especial de Lenguas	
Proceso	Descripción	Responsable
Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)

#### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa. El sistema será eliminado una vez expirado el tiempo solicitado. por medio de requerimiento.

#### Open Journal System.

#### Revista Digital Universitaria (RDU)

#### Revista de Investigación en Educación Médica (RIEM)

#### Introducción

La Revista Digital Universitaria (RDU) es una publicación electrónica bimestral de comunicación social de la ciencia, dirigida a la comunidad universitaria y al público interesado. Su principal objetivo es comunicar temas relacionados con el desarrollo de las ciencias, las humanidades, las artes y la tecnología, con la finalidad de compartir el conocimiento y despertar el interés e inquietud de sus lectores por las diversas áreas del saber. La RDU busca ser una publicación representativa de la comunidad universitaria y un referente de la comunicación social de la ciencia en México e Iberoamérica. Se distingue por poner en la mira el tema educativo dentro del desarrollo científico, humano, artístico y tecnológico. La Revista se conforma por cuatro tipos de contribuciones: artículos de comunicación social de la ciencia; artículos en los que se retoman las experiencias educativas – tanto de docentes como de estudiantes–; artículos donde se describe el quehacer universitario, tanto en la UNAM, como en distintas instituciones educativas, y contenidos de interés general que preferentemente se apoyen de material multimedia.

La revista Investigación en Educación Médica es una publicación periódica mexicana, editada trimestralmente por la Universidad Nacional Autónoma de México a través de la Facultad de Medicina, con arbitraje por pares, que pretende ser el vehículo de difusión principal en México y Latinoamérica del área de la educación en ciencias de la salud por medio de reportes de investigación original de calidad, así como artículos de revisión, de metodología, y perspectivas sobre el tema. La revista de Investigación en Educación Médica está dirigida a instituciones, académicos, profesionales y estudiantes en el campo de la medicina y ciencias de la salud

interesados en los aspectos teóricos y prácticos de la educación en este campo. Los artículos publicados se enfocan en cualquier nivel educativo, desde el pregrado, el posgrado y hasta el desarrollo profesional continuo, con el fin de analizar experiencias y estimular el establecimiento de corrientes innovadoras de pensamiento en el campo de la educación en ciencias de la salud.

## 1. INVENTARIO

<b>Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia</b>	
Identificador único	CUAIEED-DEE-013
Nombre del sistema	Open Journal System. Revista Digital Universitaria (RDU) Revista de Investigación en Educación Médica (RIEM)
Datos personales contenidos en el sistema <ul style="list-style-type: none"> <li>• Autores<sup>45</sup></li> </ul>	<ul style="list-style-type: none"> <li>• Nombre</li> <li>• Apellido paterno</li> <li>• Apellido materno</li> <li>• Correo electrónico</li> <li>• DOI</li> <li>• Nivel académico</li> <li>• Instituciones académicas</li> </ul>
<ul style="list-style-type: none"> <li>• Administrador</li> </ul>	<ul style="list-style-type: none"> <li>• Nombre</li> <li>• Apellido paterno</li> <li>• Apellido materno</li> <li>• Correo electrónico</li> </ul>
<b>Responsable:</b>	<b>Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED)</b>
Nombre:	Dr. Melchor Sánchez Mendiola
Cargo:	Coordinador de la CUAIEED
Funciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones:	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>Responsable (RDU):</b>	<b>Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente</b>
Nombre:	Mtra. María del Pilar Martínez Hernández
Cargo:	Directora de Innovación Educativa, Desarrollo Curricular y Formación Docente
Funciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones:	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>Encargados</b>	
Nombre de Encargado 2 (RDU)	Dra. De Agüero Servín María de las Mercedes
Cargo	Subdirección de Investigación en Educación
Funciones	Brindar seguimiento a los procesos de registro de usuarios (autores)
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 3	Ing. Milton Arturo García Lima
Cargo	Jefe de la Unidad de Sistemas para la Evaluación Educativa

<sup>45</sup> Los datos personales de los autores son proporcionados junto con los artículos para realizar la publicación correspondiente.

Funciones	Realizar el proceso de software con la finalidad de atender las necesidades administrativas de la DEIC garantizando que la información almacenada es veraz, oportuna y confiable
Obligaciones	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
Nombre de Encargado 4	Lic. Isaac Aboytes Morales
Cargo	Jefe de Departamento de Plataformas de Exámenes
Funciones	Realizar procesos de respaldo y restauración de la información contenida en el sistema
Obligaciones	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad (control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
Usuarios	
<b>Tipo de usuario</b>	<b>Nombre completo</b>
Administrador	Personal autorizado CUAIEED
Autores	Docentes, académicos e investigadores

## 2. ESTRUCTURA Y DESCRIPCIÓN

<b>Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia</b>	
Identificador único	CUAIEED-DEE-013
Nombre del sistema	Open Journal System. Revista Digital Universitaria (RDU) Revista de Investigación en Educación Médica (RIEM)
Tipo de soporte <sup>46</sup>	Electrónico
Descripción <sup>47</sup>	Base de datos relacional
Características del lugar donde se resguardan los soportes	El centro de datos (versión privada) es una habitación reservada para los servidores, cuenta con sistema de enfriamiento y redundancia de alimentación eléctrica. El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso. Se cuenta con circuito cerrado que graba los movimientos.

## 3. ANÁLISIS DE RIESGOS

<sup>46</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

<sup>47</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

<sup>48</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

**Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia**

Identificador único	CUAIEED-DEE-013	
Nombre del sistema	Open Journal System. Revista Digital Universitaria (RDU) Revista de Investigación en Educación Médica (RIEM)	
Riesgo	Impacto	Mitigación
Informático		
Datos de acceso comprometidos	Alto	Renovar claves de acceso
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso
Virus informático	Alto	Instalación de antivirus. Actualización constante del antivirus. Eliminar amenaza en el equipo comprometido. Plan de respaldo y recuperación.
Ataque informático	Alto	Identificar y solucionar amenaza(s) y vulnerabilidad(es). Plan de respaldo y recuperación.
Pérdida de información	Alto	Plan de respaldo y recuperación.
Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos  Lógico: revisión periódica de servicios y puertos habilitados  Monitoreo: <ul style="list-style-type: none"> <li>• Sistema de cámaras de circuito cerrado</li> <li>• Sistema de detección de intrusos</li> </ul>
Suministro e instalación eléctrica		
CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado
Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros	Alto	Se cuenta con un plan de respaldo y recuperación de información

**4. ANÁLISIS DE BRECHA**



**5. PLAN DE TRABAJO**

Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia				
Identificador único		CUAIEED-DEE-013		
Nombre del sistema		Open Journal System Revista Digital Universitaria (RDU) Revista de Investigación en Educación Médica (RIEM)		
Control	Actividades por realizar	Duración	Prioridad	Áreas responsables
Actualizaciones al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

	desarrollo para su posterior publicación			
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia	
Identificador único	CUAIEED-DEE-013
Nombre del sistema	Open Journal System. Revista Digital Universitaria (RDU) Revista de Investigación en Educación Médica (RIEM)
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital). Filtrado de paquetes desde y hacia el servidor web.

### II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El Open Journal System (OJS) no realiza tratamiento de datos personales con soportes físicos, ya que se encuentra en soporte electrónico mediante el uso de una base de datos.

### III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

### IV. REGISTRO DE INCIDENTES

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

### V. ACCESO A LAS INSTALACIONES

Información reservada

La vigilancia y el acceso físico al edificio es proporcionado por el personal de los Consejos Académicos de Área. Se cuenta con una caseta de vigilancia que registra todos los accesos para el ingreso a la Dirección de Evaluación Educativa (DEE).

Para el acceso a la DEE cuenta con un lector biométrico de huella digital, el acceso al Centro de Datos está restringido únicamente al personal autorizado de la USEE (cuenta con llave) y además tiene instalado un sistema de circuito cerrado con detección de movimiento.

## VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

## VII. PERFILES DE USUARIO Y CONTRASEÑA

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hacks* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

## XI. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia		
Identificador único	CUAIEED-DEE-013	
Nombre del sistema	Open Journal System Revista Digital Universitaria (RDU) Revista de Investigación en Educación Médica (RIEM)	
Recurso	Descripción	Control
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades.  Se realiza un escaneo de puertos de manera periódica con el fin de corroborar que solo estén abiertos los puertos necesarios por la aplicación.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones.
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales.	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario autorizado por la DEE (archivo cifrado con protección de contraseña).

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

## 9. MEJORA CONTINUA

*No aplica.*

### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia			
Identificador único	CUAIEED-DEE-013		
Nombre del sistema	Open Journal System. Revista Digital Universitaria (RDU) Revista de Investigación en Educación Médica (RIEM)		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia			
Identificador único	CUAIEED-DEE-013		
Nombre del sistema	Open Journal System. Revista Digital Universitaria (RDU) Revista de Investigación en Educación Médica (RIEM)		
Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia		
Identificador único	CUAIEED-DEE-013	
Nombre del sistema	Open Journal System. Revista Digital Universitaria (RDU) Revista de Investigación en Educación Médica (RIEM)	
Proceso	Descripción	Responsable
Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los respaldos automatizados se resguardan de manera indefinida	Unidad de Sistemas para la Evaluación Educativa (USEE)

### 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia
---



Identificador único	CUAIEED-DEE-013	
Nombre del sistema	Open Journal System. Revista Digital Universitaria (RDU) Revista de Investigación en Educación Médica (RIEM)	
Proceso	Descripción	Responsable
Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa. El sistema será eliminado una vez expirado el tiempo solicitado. por medio de requerimiento.

### Plataforma LimeSurvey Seguimiento de egresados

#### Introducción

Plataforma utilizada para la aplicación de instrumentos en línea para el seguimiento de estudiantes egresados de las diferentes facultades y escuelas de la universidad.

#### 1. INVENTARIO

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-014
Nombre del sistema	Plataforma LimeSurvey Seguimiento de egresados
Datos personales contenidos en el sistema <ul style="list-style-type: none"> <li>Participantes<sup>49</sup></li> </ul>	<i>Los datos solicitados dependen de la finalidad del instrumento</i> <ul style="list-style-type: none"> <li>Nombre</li> <li>Apellido paterno</li> <li>Apellido materno</li> <li>Nacionalidad</li> <li>Domicilio</li> <li>Correo Electrónico</li> <li>Teléfono fijo o móvil</li> <li>RFC</li> <li>CURP</li> </ul>
<b>Responsable:</b>	<b>Dirección de Evaluación Educativa</b>
Nombre:	Dr. Adrián Martínez
Cargo:	Director de Evaluación Educativa
Funciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.

<sup>49</sup> Los datos personales serán recabados de forma directa cuando el participante los proporciona al momento de registrarse.

Obligaciones:	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>Encargados</b>	
Nombre de Encargado 2	Mtra. Laura Elena Rojo Chávez
Cargo	Subdirectora de Evaluación de Procesos y Programas Académicos
Funciones	Brindar seguimiento a los procesos de registro de participantes
Obligaciones	Cumplir con la obligación legal de resguardar los datos personales
Nombre de Encargado 3	Ing. Milton Arturo García Lima
Cargo	Jefe de la Unidad de Sistemas para la Evaluación Educativa
Funciones	Realizar el proceso de software con la finalidad de atender las necesidades administrativas de la DEE garantizando que la información almacenada es veraz, oportuna y confiable
Obligaciones	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
Nombre de Encargado 4	Lic. Isaac Aboytes Morales
Cargo	Jefe de Departamento de Plataformas de Exámenes
Funciones	Realizar procesos de respaldo y restauración de la información contenida en el sistema
Obligaciones	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad (control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
<b>Usuarios</b>	
<b>Tipo de usuario</b>	<b>Nombre completo</b>
Participantes	Docentes y académicos de la UNAM

## 2. ESTRUCTURA Y DESCRIPCIÓN

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-014
Nombre del sistema	Plataforma LimeSurvey Seguimiento de egresados
Tipo de soporte <sup>50</sup>	Electrónico
Descripción <sup>51</sup>	Base de datos relacional
Características del lugar donde se resguardan los soportes	El centro de datos (versión privada) es una habitación reservada para los servidores, cuenta con sistema de enfriamiento y redundancia de alimentación eléctrica.

<sup>50</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

<sup>51</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

<sup>52</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros)

El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso.  
Se cuenta con circuito cerrado que graba los movimientos

### 3. ANÁLISIS DE RIESGOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-014	
Nombre del sistema	Plataforma LimeSurvey Seguimiento de egresados	
Riesgo	Impacto	Mitigación
Informático		
Datos de acceso comprometidos	Alto	Renovar claves de acceso
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso
Virus informático	Alto	Instalación de antivirus. Actualización constante del antivirus. Eliminar amenaza en el equipo comprometido. Plan de respaldo y recuperación.
Ataque informático	Alto	Identificar y solucionar amenaza(s) y vulnerabilidad(es). Plan de respaldo y recuperación.
Pérdida de información	Alto	Plan de respaldo y recuperación.
Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos.  Lógico: revisión periódica de servicios y puertos habilitados.  Monitoreo: <ul style="list-style-type: none"> <li>• Sistema de cámaras de circuito cerrado</li> <li>• Sistema de detección de intrusos</li> </ul>
Suministro e instalación eléctrica		
CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado
Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros	Alto	Se cuenta con un plan de respaldo y recuperación de información

### 4. ANÁLISIS DE BRECHA

del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.  
En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-014	
Nombre del sistema	Plataforma LimeSurvey Seguimiento de egresados	
Nombre	Causa	Solución
Actualizaciones al sistema operativo	No actualizar el sistema operativo	Actualizaciones periódicas a los sistemas operativos
Actualizaciones la plataforma de desarrollo	Compatibilidad con las versiones de producción. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación
Servidores web y de aplicaciones	Compatibilidad con las versiones de producción de sistemas operativos y librerías. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación
Cuentas de acceso en desuso	Término de relación laboral del personal asignado Falta de notificación al área para realizar la restricción de acceso correspondiente	Revisión periódica de cuentas de usuarios vigentes
Asignación errónea de privilegios de usuario	Equivocación en la creación de cuentas de usuario. Solicitud de cambios en los privilegios en las cuentas de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario
Capacitación a usuarios	Falta de capacitación a usuarios que provoque la falta de confiabilidad en la integridad de la información (nuevos usuarios y/o cambios de rol de usuarios)	Capacitar adecuadamente al personal para los roles asignados
Flujo de la información	Solicitud de omisión de procesos durante el flujo de información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema

## 5. PLAN DE TRABAJO

Dirección de Evaluación Educativa				
Identificador único	CUAIEED-DEE-014			
Nombre del sistema	Plataforma LimeSurvey Seguimiento de egresados			
Control	Actividades por realizar	Duración	Prioridad	Áreas responsables
Actualizaciones al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

	controlado para su posterior publicación			
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Evaluación Educativa	
Identificador único	CUAIEED-DEE-014
Nombre del sistema	LimeSurvey Seguimiento de egresados
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital). Filtrado de paquetes desde y hacia el servidor web.

### II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Los instrumentos almacenados por la plataforma LimeSurvey no realizan tratamiento de datos personales con soportes físicos, ya que se encuentran en soporte electrónico mediante el uso de una base de datos.

### III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

### IV. REGISTRO DE INCIDENTES

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

## V. ACCESO A LAS INSTALACIONES

La vigilancia y el acceso físico al edificio es proporcionado por el personal de los Consejos Académicos de Área. Se cuenta con una caseta de vigilancia que registra todos los accesos para el ingreso a la Dirección de Evaluación Educativa (DEE).

Para el acceso a la DEE cuenta con un lector biométrico de huella digital, el acceso al Centro de Datos está restringido únicamente al personal autorizado de la USEE (cuenta con llave) y además tiene instalado un sistema de circuito cerrado con detección de movimiento.

## VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

## VII. PERFILES DE USUARIO Y CONTRASEÑA

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hacks* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

## XI. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-014	
Nombre del sistema	Plataforma LimeSurvey	
Recurso	Seguimiento de egresados	
Herramientas automatizadas	Descripción	Control
	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades.  Se realiza un escaneo de puertos de manera periódica con el fin de corroborar que solo estén abiertos los puertos necesarios por la aplicación.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones.
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales.	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

## 9. MEJORA CONTINUA

*No aplica*

### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-014		
Nombre del sistema	Plataforma LimeSurvey Seguimiento de egresados		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-014		
Nombre del sistema	Plataforma LimeSurvey Seguimiento de egresados		
Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-014	
Nombre del sistema	Plataforma LimeSurvey Seguimiento de egresados	
Proceso	Descripción	Responsable
Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los respaldos automatizados se resguardan de manera indefinida	Unidad de Sistemas para la Evaluación Educativa (USEE)

### 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-014	
Nombre del sistema	Plataforma LimeSurvey Seguimiento de egresados	
Proceso	Descripción	Responsable

Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)
----------------	--	--

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa. El sistema será eliminado una vez expirado el tiempo solicitado. por medio de requerimiento.

### Plataforma WordPress. Comunidad de Educación Basada en Evidencias

#### Introducción

Contribuir en la toma de decisiones educativas a nivel micro, meso y macro, fundamentadas en resultados de investigación científica, a través de la construcción de una comunidad que practique la Educación Basada en Evidencias dentro de su ejercicio profesional en el ámbito educativo, para compartir experiencias y diseminar propuestas de aplicación dentro y fuera de la Universidad.

#### 1. INVENTARIO

<b>Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente</b>	
Identificador único	CUAIEED-DEE-015
Nombre del sistema	Plataforma WordPress Comunidad de Educación Basada en Evidencias (CEBE)
Datos personales contenidos en el sistema <ul style="list-style-type: none"> <li>Participantes<sup>53</sup></li> </ul>	<i>Los datos solicitados dependen de la finalidad del instrumento</i> <ul style="list-style-type: none"> <li>Nombre</li> <li>Apellido paterno</li> <li>Apellido materno</li> <li>Correo Electrónico</li> <li>RFC</li> <li>CURP</li> </ul>

<b>Responsable:</b>	<b>Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (CUAIEED)</b>
Nombre:	Dr. Melchor Sánchez Mendiola
Cargo:	Coordinador de la CUAIEED
Funciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones:	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
<b>Responsable:</b>	<b>Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente</b>

<sup>53</sup> Los datos personales serán recabados de forma directa cuando el participante los proporciona al momento de registrarse.



Nombre:	Mtra. María del Pilar Martínez Hernández
Cargo:	Directora de Innovación Educativa, Desarrollo Curricular y Formación Docente
Funciones:	Decidir sobre el tratamiento de los datos personales, así como el contenido, finalidad y uso del sistema.
Obligaciones:	Vigilar que los procesos cumplan con todas las medidas de seguridad física y administrativa.
Encargados	

Nombre de Encargado 3	Ing. Milton Arturo García Lima
Cargo	Jefe de la Unidad de Sistemas para la Evaluación Educativa
Funciones	Realizar el proceso de software con la finalidad de atender las necesidades administrativas de la DEE garantizando que la información almacenada es veraz, oportuna y confiable
Obligaciones	Resguardo de la información contenida en el sistema mediante mecanismos de seguridad (control de acceso)
Nombre de Encargado 4	Lic. Isaac Aboytes Morales
Cargo	Jefe de Departamento de Plataformas de Exámenes
Funciones	Realizar procesos de respaldo y restauración de la información contenida en el sistema
Obligaciones	Resguardo de la información contenida en las bases de datos del sistema mediante mecanismos de seguridad (control de acceso lógico y físico), monitoreo de redes, detección de incidentes y/o fallas en los equipos
Usuarios	
<b>Tipo de usuario</b>	<b>Nombre completo</b>
Participantes	Docentes de educación media superior y superior

## 2. ESTRUCTURA Y DESCRIPCIÓN

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único	CUAIEED-DEE-015
Nombre del sistema	Plataforma WordPress Comunidad de Educación Basada en Evidencias (CEBE)
Tipo de soporte <sup>54</sup>	Electrónico
Descripción <sup>55</sup>	Base de datos relacional
Características del lugar donde se resguardan los soportes	El sistema de información se resguarda en una plataforma habilitada reservada para el uso exclusivo del sistema de enseñanza y aprendizaje.

<sup>54</sup> En caso de que el área universitaria prevea cambiar el tipo de soporte que utiliza el por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

<sup>55</sup> Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

<sup>56</sup> Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

- Para soportes físicos, el área universitaria deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción ofrecida por el área universitaria deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes.

El acceso físico es mediante una chapa a la cual solo personal de la USEE tiene acceso. Se cuenta con circuito cerrado que graba los movimientos

### 3. ANÁLISIS DE RIESGOS

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único	CUAIEED-DEE-015	
Nombre del sistema	Plataforma WordPress Comunidad de Educación Basada en Evidencias (CEBE)	
Riesgo	Impacto	Mitigación
Informático		
Datos de acceso comprometidos	Alto	Renovar claves de acceso
Divulgación de información	Alto	Suspensión de acceso al sistema
Extravío de datos de acceso	Alto	Renovar claves de acceso
Virus informático	Alto	Instalación de antivirus. Actualización constante del antivirus. Eliminar amenaza en el equipo comprometido. Plan de respaldo y recuperación.
Ataque informático	Alto	Identificar y solucionar amenaza(s) y vulnerabilidad(es). Plan de respaldo y recuperación.
Pérdida de información	Alto	Plan de respaldo y recuperación.
Control de acceso	Alto	Físico: acceso a las instalaciones mediante caseta de vigilancia a la dependencia por medio de control biométrico y al centro de datos  Lógico: revisión periódica de servicios y puertos habilitados  Monitoreo: <ul style="list-style-type: none"> <li>• Sistema de cámaras de circuito cerrado</li> <li>• Sistema de detección de intrusos</li> </ul>
Suministro e instalación eléctrica		
CFE	Alto	Se cuenta con un sistema de respaldo UPS y una planta eléctrica
UPS	Alto	Mantenimiento preventivo semestral para evaluar el estado
Variación de voltaje	Alto	Se cuenta con un sistema de respaldo UPS
Planta eléctrica	Alto	Mantenimiento preventivo semestral para evaluar el estado
Desastre natural		
Tormenta eléctrica, sismo, inundación, entre otros	Alto	Se cuenta con un plan de respaldo y recuperación de información

### 4. ANÁLISIS DE BRECHA

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente

En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

Identificador único	CUAIEED-DEE-015	
Nombre del sistema	Plataforma WordPress Comunidad de Educación Basada en Evidencias (CEBE)	
Nombre	Causa	Solución
Actualizaciones al sistema operativo	No actualizar el sistema operativo	Actualizaciones periódicas a los sistemas operativos
Actualizaciones la plataforma de desarrollo	Compatibilidad con las versiones de producción. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación
Servidores web y de aplicaciones	Compatibilidad con las versiones de producción de sistemas operativos y librerías. No se cuenta con la última versión disponible	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente de desarrollo para su posterior publicación
Cuentas de acceso en desuso	Término de relación laboral del personal asignado Falta de notificación al área para realizar la restricción de acceso correspondiente	Revisión periódica de cuentas de usuarios vigentes
Asignación errónea de privilegios de usuario	Equivocación en la creación de cuentas de usuario. Solicitud de cambios en los privilegios en las cuentas de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario
Capacitación a usuarios	Falta de capacitación a usuarios que provoque la falta de confiabilidad en la integridad de la información (nuevos usuarios y/o cambios de rol de usuarios)	Capacitar adecuadamente al personal para los roles asignados
Flujo de la información	Solicitud de omisión de procesos durante el flujo de información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema

## 5. PLAN DE TRABAJO

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente				
Identificador único	CUAIEED-DEE-015			
Nombre del sistema	Plataforma WordPress Comunidad de Educación Basada en Evidencias (CEBE)			
Control	Actividades por realizar	Duración	Prioridad	Áreas responsables
Actualizaciones al sistema operativo	Actualizaciones periódicas a los sistemas operativos	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Actualizaciones la plataforma de desarrollo	Análisis y prueba de actualizaciones a la plataforma de desarrollo ( <i>framework</i> ) en un ambiente controlado para su posterior publicación	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Servidores web y de aplicaciones	Análisis y prueba de actualizaciones de sistemas operativos y librerías en un ambiente	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

	de desarrollo para su posterior publicación			
Cuentas de acceso en desuso	Revisión periódica de cuentas de usuarios vigentes	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Asignación errónea de privilegios de usuario	Revisión periódica y ajustes de privilegios en las cuentas de usuario	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Capacitación a usuarios	Capacitar adecuadamente al personal para los roles asignados	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa
Flujo de la información	Cumplir con los flujos de información establecidos en el manual de procesos y uso del sistema	Tarea continua	Alta	Unidad de Sistemas para la Evaluación Educativa

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente	
Identificador único	CUAIEED-DEE-015
Nombre del sistema	Plataforma WordPress Comunidad de Educación Basada en Evidencias (CEBE)
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante el traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante el traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Implementación de comunicación cifrada en la comunicación cliente-servidor (certificado digital). Filtrado de paquetes desde y hacia el servidor web.

### II. RESGUARDO DE DATOS PERSONALES CON SOPORTES FÍSICOS

La plataforma WordPress no realiza tratamiento de datos personales con soportes físicos, ya que se encuentran en soporte electrónico mediante el uso de una base de datos.

### III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Las bitácoras, archivos de log y registros de servidores de aplicaciones y de bases de datos, así como los eventos y operaciones realizadas dentro de la plataforma, se almacenan en formato electrónico.

### IV. REGISTRO DE INCIDENTES

Los incidentes son reportados a la Unidad de Sistemas para la Evaluación Educativa (USEE) donde se realiza un análisis de las bitácoras para determinar la gravedad de la incidencia y determinar su solución.

### V. ACCESO A LAS INSTALACIONES

Información reservada

La vigilancia y el acceso físico al edificio es proporcionado por el personal de los Consejos Académicos de Área. Se cuenta con una caseta de vigilancia que registra todos los accesos para el ingreso a la Dirección de Evaluación Educativa (DEE).

Para el acceso a la DEE cuenta con un lector biométrico de huella digital, el acceso al Centro de Datos está restringido únicamente al personal autorizado de la USEE (cuenta con llave) y además tiene instalado un sistema de circuito cerrado con detección de movimiento.

## VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

El procedimiento para actualizar o corregir datos personales es mediante solicitud expresa del usuario y autorización del responsable del sistema.

## VII. PERFILES DE USUARIO Y CONTRASEÑA

El modelo de control de acceso a las plataformas se encuentra basado en roles (perfiles). Las contraseñas asignadas a los usuarios tienen la característica de ser robustas, tratando de evitar *hacks* basados en diccionarios, ataques de fuerza bruta, suplantación de identidad o filtración de datos existentes.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se generan copias periódicas de la información alojada en la plataforma. Una vez identificada la incidencia, su impacto e información comprometida, se procede a la recuperación en función de la fecha del evento.

## XI. PLAN DE CONTINGENCIA

Se cuenta con un plan de contingencia que permite la continuidad de operación de la plataforma, el cual utiliza como principal insumo los respaldos periódicos generados y alojados en medios digitales. También se cuentan con sistemas espejo de los aplicativos para asegurar la operación.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Dirección de Innovación Educativa, Desarrollo Curricular y Formación Docente		
Identificador único	CUAIEED-DEE-015	
Nombre del sistema	Plataforma WordPress Comunidad de Educación Basada en Evidencias (CEBE)	
Recurso	Descripción	Control
Herramientas automatizadas	Se utilizan diversas herramientas para realizar pruebas de penetración y escaneo de puertos abiertos.	Se realizan pruebas de penetración periódicamente con el fin de identificar y mitigar posibles vulnerabilidades.  Se realiza un escaneo de puertos de manera periódica con el fin de corroborar que solo estén abiertos los puertos necesarios por la aplicación.
Bitácora del sistema	Revisión aleatoria	Revisar de manera regular la bitácora con el fin de indagar si hubiera algún uso o comportamiento inusual en la aplicación mediante el análisis de excepciones.
Correo electrónico	Envío de reportes mediante correos electrónicos institucionales.	Los reportes que contienen datos personales son enviados directamente al buzón de correo electrónico del usuario autorizado por la DEE (archivo cifrado con protección de contraseña).

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Cada nuevo usuario que se incorpora a la CUAIEED y en el uso de o los sistemas, es capacitado por personal de su área de adscripción indicando las medidas de seguridad, monitoreo y control de acceso correspondientes.

## 9. MEJORA CONTINUA

No aplica

### 9.1. ACTUALIZACIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Dirección de Evaluación Educativa			
Identificador único	Plataforma WordPress Comunidad de Educación Basada en Evidencias (CEBE)		
Nombre del sistema	CUAIEED-DEE-015		
Actividad	Descripción	Duración	Cobertura
Actualización de sistemas operativos y versiones de plataforma	Proceso de actualización de sistemas operativos y versiones de plataforma	15 días	Total

### 9.2. ACTUALIZACIÓN Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Dirección de Evaluación Educativa			
Identificador único	CUAIEED-DEE-015		
Nombre del sistema	Plataforma WordPress Comunidad de Educación Basada en Evidencias (CEBE)		
Actividad	Descripción	Duración	Cobertura
Reparación o reemplazo del servidor (hardware)	Reparación o reemplazo del servidor en caso de fallo	Por evento	Total

### 9.3. PROCESOS PARA LA CONSERVACIÓN, PRESERVACIÓN Y RESPALDOS DE INFORMACIÓN

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-015	
Nombre del sistema	Plataforma WordPress Comunidad de Educación Basada en Evidencias (CEBE)	
Proceso	Descripción	Responsable
Resguardo de unidades de almacenamiento	Las unidades de almacenamiento donde se realizan los respaldos automatizados se resguardan de manera indefinida	Unidad de Sistemas para la Evaluación Educativa (USEE)

### 9.4. PROCESOS DE BORRADO SEGURO Y DISPOSICIÓN FINAL DE EQUIPOS Y COMPONENTES INFORMÁTICOS

Dirección de Evaluación Educativa		
Identificador único	CUAIEED-DEE-015	
Nombre del sistema	Plataforma WordPress Comunidad de Educación Basada en Evidencias (CEBE)	
Proceso	Descripción	Responsable
Borrado seguro	Formato de bajo nivel cuando se reasigna el equipo Destrucción del disco cuando es baja definitiva del equipo	Unidad de Sistemas para la Evaluación Educativa (USEE)

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Realizar solicitud de baja del aplicativo o software que ya no se utiliza, indicando el tiempo que debe seguir funcionando la plataforma antes de ser eliminada, y en caso de ser necesario, indicar el tipo de entregable. La petición debe ser realizada vía oficio a la Unidad de Sistemas para la Evaluación Educativa. El sistema será eliminado una vez expirado el tiempo solicitado. Por medio de requerimiento.

### Sistema Institucional de Compras

#### Introducción

Con base en el Plan de Desarrollo Institucional 2015-2019, se proyectó la línea de acción 7.4, aplicación de las TIC'S en los procesos de gestión administrativa, que refiere a simplificar la administración universitaria creando el Sistema Institucional de Compras. Por lo anterior, se asignó la tarea a la Dirección General de Proveeduría de desarrollar y administrar dicho Sistema. Será responsabilidad de dicha Dirección, así como de cada una de las entidades y dependencias en el ámbito de sus atribuciones, mantenerlo actualizado.

#### Beneficios

Proporcionar una herramienta administrativa enfocada a apoyar:

- En la eficiencia de las adquisiciones arrendamientos y servicios de la UNAM.
- Prevenir y apoyar en el cumplimiento de la normatividad
- En la colaboración institucional entre el patronato y las distintas dependencias centralizadoras que, por la naturaleza de sus funciones, intervienen en alguna etapa del procedimiento de contratación.
- En la gestión logrando disminuir los tiempos de servicio, mediante la integración de sistemas institucionales.
- Al utilizar un sistema de gestión y la firma electrónica avanzada como un mecanismo de seguridad y simplificación de las autorizaciones se disminuye de manera considerable el uso excesivo de papel en los trámites.

### 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Departamento de Bienes y Suministros	
Identificador único*	UNAM:6C.13/482-63"2022"
Nombre del sistema A1*:	Sistema Institucional de Compra (SIC)
Datos personales (sensibles o no) contenidos en el sistema*:	Nombres, correos electrónicos (institucional), firmas electrónicas y autógrafas, datos del proveedor

Responsable*:	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
Nombre*:	Lic. Ximena Vázquez Rodríguez
Cargo*:	Jefa del Departamento de Bienes y Suministros
Funciones*:	Vigilar la adquisición de bienes e insumos requeridos para las diferentes áreas a través de la Dirección General de Proveduría, o en su caso, a través de compra directa con el proveedor, de acuerdo a la normatividad en materia de adquisiciones, arrendamiento y servicios de la UNAM, y en materia administrativa para dependencias universitarias.
Obligaciones*:	<p>Revisar las Solicitudes Internas de Compra generadas por los Solicitantes.</p> <p>Generar Solicitudes de Compra de acuerdo al procedimiento indicado en la normatividad vigente.</p> <p>Cotizar, generar cuadros comparativos y estudios de mercado de los bienes y servicios solicitados.</p> <p>Aprobar y firmar electrónicamente las Solicitudes de Compra.</p> <p>Generar pedidos.</p>
	Usuarios:
(Nombre del Usuario *)	Directores, Subdirectores, Coordinadores, Secretarios Administrativo y Técnico, Jefes de Unidad, Jefes de Departamento, Responsables de proyectos PAPIIT y PAPIME Asistentes, Proveedores
Cargo*:	Funcionarios, Académicos y Confianza
Funciones*:	<p>Capturar/Generar Solicitudes Internas de Compra</p> <p>Aprobar y Firmar electrónicamente las Solicitudes Internas de Compra.</p>



Obligaciones*:	Registrar las Solicitudes Internas de Compra en el SIC.
----------------	---

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Departamento de Bienes y Suministros	
Identificador único*	UNAM:6C.13/482-63"2022"
(Nombre del sistema A1*)	Sistema Institucional de Compras (SIC)
Tipo de soporte: *	Electrónico y documentos físicos
Descripción: *	Expedientes y base de datos
Características del lugar donde se resguardan los soportes: *	Se resguardan las carpetas en el Departamento de Bienes y Suministros en un mueble que cuenta con llave y en electrónico en la computadora de la Jefa del Departamento de Bienes y Suministros la cual tiene contraseña.

## 3. ANÁLISIS DE RIESGOS

Departamento de Bienes y Suministros		
Identificador único	UNAM:6C.13/482-63"2022"	
(Nombre del sistema A1)	Sistema Institucional de Compras (SIC)	
Riesgo	Impacto	Mitigación

Ingreso no autorizado al Departamento de Bienes y Suministros	Medio	Uso de contraseñas seguras cámaras y cerraduras
Fuga de información	Medio	Sólo personal autorizado es el que tiene acceso a la información

#### 4. ANÁLISIS DE BRECHA

Departamento de Bienes y Suministros		
Identificador único*	UNAM:6C.13/482-63"2022"	
Nombre del sistema A1) *	Sistema Institucional de Compras (SIC)	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Identificación y autenticación	Se requiere de un usuario y contraseña para ingresar al sistema y llaves para abrir los muebles	Uso de contraseñas y llaves
Identificación y calificación del personal encargado	Identificar al personal autorizado para realizar trámites en el SIC	Uso de firmas electrónicas sólo de Funcionarios

#### 5. PLAN DE TRABAJO

Departamento de Bienes y Suministros	
Identificador único*	UNAM:6C.13/482-63"2022"

(Nombre del sistema A1) *	Sistema Institucional de Compras (SIC)		
Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Departamento de Bienes y Suministros	
Identificador único*	UNAM:6C.13/482-63"2022"
(Nombre del sistema A1) *	Sistema Institucional de Compras (SIC)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	El envío de la información con los proveedores se realiza por correo electrónico institucional y el envío de la información en el SIC
Transferencias mediante el traslado de soportes electrónicos:	Las cotizaciones no se encuentran cifradas
Transferencias mediante el traslado sobre redes electrónicas:	Se utiliza red privada en la CUAIEED

### II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Se cuenta con cámaras de vigilancia, cerraduras en puertas, así como cerradura en el mueble en el que se resguardan los documentos físicos.

Nombre	Cargo	Funciones	Obligaciones
Lic. Ximena Vázquez Rodríguez	Jefa del Departamento de Bienes y Suministros	Vigilar la adquisición de bienes e insumos requeridos para las diferentes áreas a través de la Dirección General de Proveeduría, o, en su caso, a través de compra directa con el proveedor, de acuerdo a la normatividad en materia de adquisiciones, arrendamiento y servicios de la UNAM, y en materia administrativa para dependencias universitarias.	Revisar las Solicitudes Internas de Compra generadas por los Solicitantes. Generar Solicitudes de Compra de acuerdo al procedimiento indicado en la normatividad vigente. Cotizar, generar cuadros comparativos y estudios de mercado de los bienes y servicios solicitados. Aprobar y firmar electrónicamente las Solicitudes de Compra. Generar pedidos.

### III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No podemos tener un control debido a que nosotros no somos responsables de administrar el servidor.

### IV. REGISTRO DE INCIDENTES

En la cuestión electrónica no podemos tener control en caso de que exista un incidente, sin embargo, en la cuestión de la documentación física se mantiene la documentación bajo llave.

### V. ACCESO A LAS INSTALACIONES

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente y se asigna un gafete. La dependencia se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso.

(exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el director de la Dirección de Desarrollo de Sistemas para la Educación.

## VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No contamos tenemos los permisos para agregar o quitar datos personales de ninguno de los usuarios registrados en el SIC.

## VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los roles del usuario que se manejan en el SIC son establecidos por los desarrolladores de este, la jefa del Departamento de Bienes y Suministros da de alta a los nuevos usuarios, con base en lo que indique el responsable de cada área.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

La Dirección General de Proveduría es la encargada de respaldar y recuperar datos del SIC.

## IX. PLAN DE CONTINGENCIA

La Dirección General de Proveduría es la responsable de desarrollar un plan de contingencia del SIC.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Departamento de Bienes y Suministros		
Identificador único*	UNAM:6C.13/482-63/2022	
Nombre del sistema A1)	Sistema Institucional de Compras (SIC)	
Recurso*	Descripción*	Control*
No aplica	No aplica	No aplica

### 7.2 Procedimiento para la revisión de las medidas de seguridad

Departamento de Bienes y Suministros		
Identificador único*	UNAM:6C.13/482-63"2022"	
(Nombre del sistema A1) *	Sistema Institucional de Compras (SIC)	
Medida de seguridad*	Procedimiento*	Responsable*
No aplica	No aplica.	Dirección General de Proveeduría

### 7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Departamento de Bienes y Suministros		
Identificador único*	UNAM:6C.13/482-63"2022"	
(Nombre del sistema A1) *	Sistema Institucional de Compras (SIC)	
Medida de seguridad*	Resultado de evaluación*	Responsable*
No aplica	No aplica	Dirección General de Proveeduría

### 7.4 Acciones para la corrección y actualización de las medidas de seguridad

Departamento de Bienes y Suministros	
Identificador único*	UNAM:6C.13/482-63"2022"
(Nombre del sistema A1) *	Sistema Institucional de Compras (SIC)

Medida de seguridad*	Acciones*	Responsable*
No aplica	No aplica	Dirección General de Proveeduría

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

### 8.1 Programa de capacitación a los responsables de seguridad de datos personales

La Dirección General de Proveeduría es la encargada de impartir las capacitaciones del sistema

### 8.2 Programa de difusión de la protección a los datos personales

No se tiene un programa de difusión de la protección a los datos personales

## 9. MEJORA CONTINUA

### 9.1 Actualización y mantenimiento de sistemas de información

Departamento de Bienes y Suministros			
Identificador único*	UNAM:6C.13/482-63"2022"		
(Nombre del sistema A1) *	Sistema Institucional de Compras (SIC)		
Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

### 9.2 Actualización y mantenimiento de equipo de cómputo

Departamento de Bienes y Suministros			
Identificador único*	UNAM:6C.13/482-63"2022"		
(Nombre del sistema A1*:	Sistema Institucional de Compras (SIC)		
Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

### 9.3 Procesos para la conservación, preservación y respaldos de información

Departamento de Bienes y Suministros		
Identificador único*	UNAM:6C.13/482-63"2022"	
(Nombre del sistema A1*:	Sistema Institucional de Compras (SIC)	
Proceso*	Descripción*	Responsable*
No aplica	No aplica	Dirección General de Proveeduría

### 9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Departamento de Bienes y Suministros	
Identificador único*	UNAM:6C.13/482-63"2022"



(Nombre del sistema A1*:	Sistema Institucional de Compras (SIC)	
Proceso*	Descripción*	Responsable*
No aplica	No aplica	Dirección General de Proveeduría

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No aplica

### **Sistema Integral de Personal**

#### **Introducción**

El Sistema Integral de Personal es un sistema centralizado y desarrollado por la Dirección de Sistemas de la Dirección General de Personal de la UNAM, a través del cual los diferentes Departamentos de Personal de la UNAM incluyendo el de la CUAIEED, operamos los siguientes trámites:

- Contratación de personal
- Trámite de licencias médicas, sin sueldo menores y mayores a 30 días, licencias sindicales.
- Movimientos de personal: Altas, Bajas, Otros nombramientos, Renuncias, Defunciones, Cambios de horario, Definitividad, Art. 51 del EPA, interinatos, laudos, permutas, reanudación de labores, reinstalaciones, reclasificaciones, retabulaciones, revocaciones, término de nombramientos,
- Promoción personal administrativo de Base
- Oficio Certificación / Diferimiento para Personal Académico
- Solicitud Programa de Retiro por Jubilación / Pensión
- Solicitud de Certificación Jubilación / Pensión
- Oficio de Solicitud de Cobertura de plaza personal administrativo de Base
- Designación de Beneficiarios para Pago de Marcha
- Solicitud de Pago de Ayuda de Guardería
- Solicitud de Cambio de Domicilio
- Solicitud de Credencial
- Ropa de Trabajo
- Autorización de Contratos y Adendas
- Autorización de Notificaciones
- Constancias de Empleo y Sueldo
- Seguimiento Relaciones DGAPA
- Generación de Carta de Confidencialidad

## Beneficios

- Simplificar los trámites administrativos que deriven de los movimientos de personal académico, administrativo de confianza, base y funcionarios.
- Al utilizar un sistema de gestión y la firma electrónica avanzada como un mecanismo de seguridad y simplificación de las autorizaciones se disminuye de manera considerable el uso excesivo de papel en los trámites.

## 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Departamento de Personal	
Identificador único*	Sistema Integral de Personal (SIP)
Nombre del sistema A1*:	Sistema Integral de Personal (SIP)
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, RFC, CURP, edad, género, fecha de nacimiento, domicilio, teléfono, beneficiarios, número de empleado, número de sueldo, categoría, área de trabajo, jornada y horario laboral, histórico de incidencias, licencias, y promociones escalafonarias,
Responsable*:	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
Nombre*:	Lic. Erika Patricia Quintero Herrera
Cargo*:	Jefa del Departamento de Personal
Funciones*:	Atender, efectuar y registrar los movimientos administrativos del personal adscrito en la Coordinación en materia de derechos, prestaciones y servicios que correspondan, acorde a la normatividad vigente, así como a la Legislación Universitaria y al Sistema de Gestión de la Calidad.
Obligaciones*:	Organizar, dirigir y supervisar las actividades del Departamento, desde la elaboración hasta la ejecución de las gestiones. Revisar el cumplimiento de las normas y procedimientos generales de la Institución, así como aplicar las políticas y normas específicas establecidas en el Instituto. Establecer comunicación con instancias internas y externas a la Coordinación, a fin de desarrollar las gestiones propias del Departamento. Verificar que el personal de nuevo ingreso a la dependencia cumpla con los requisitos establecidos por la normatividad aplicable.

Atender asuntos que se deriven de la contratación del personal adscrito a la Coordinación.

Mantener actualizada la plantilla del personal, conforme a la estructura organizacional de la Institución.

Atender y orientar al personal administrativo y académico en asuntos relativos a trámites y procedimientos administrativos.

Evaluar el desempeño del personal a su cargo y promover su actualización.

Organizar la inscripción de los Programas de Estímulos por puntualidad y asistencia, de Calidad y Eficiencia del personal Administrativo de Base y del Programa EDPAC, conforme a las normas establecidas.

Emitir el pago de la nómina desde su recepción hasta la devolución.

Operar, supervisar y observar que los trámites de los movimientos de altas, bajas y cambios de adscripción del personal de la Entidad, se realicen conforme a la normatividad universitaria en vigor, con el propósito de administrar eficazmente la plantilla del personal administrativo de base, confianza, funcionarios y honorarios.

Definir, establecer y supervisar los mecanismos internos para el pago oportuno de las remuneraciones y prestaciones a las que tiene derecho el personal (guardería, tiempo extra, Estímulos al Desempeño del Personal Administrativo de Confianza, Programa de Calidad y Eficiencia del Personal de Base, Cláusula 68, Ropa de Trabajo y trámites de prestaciones varias).

Colaborar en las actividades de revisión por la dirección específica, de auditorías internas y externas y dar seguimiento a las acciones preventivas, correctivas o de mejora y del servicio no conforme.

Participar como Representante del Secretario Administrativo ante el Sistema de Gestión de la Calidad, con las siguientes actividades:

Vigilar y asegurar que el personal de cada departamento cumpla las disposiciones de control de documentos del Sistema de Gestión de la Calidad.

Identificar las necesidades de recursos y proponer cambios al Sistema de Gestión de la Calidad.

Enviar los informes solicitados por la Dirección General de Servicios Administrativos (DGSA).

Registrar, controlar, calcular y graficar de la información correspondiente a la medición de los indicadores del Sistema de Gestión de la Calidad de la Coordinación.

Coordinar y dar seguimiento a las reuniones de análisis de los resultados y de medición de los

	<p>indicadores de las auditorías de calidad establecidas por la DGSA.</p> <p>Apoyar la ejecución de las Auditorías de Calidad en la Coordinación</p> <p>Apoyar en el diseño, difusión de materiales y la actualización de formatos del Sistema de Gestión de la Calidad.</p> <p>Proporcionar a la Secretaría Administrativa los informes de los procesos.</p> <p>Aplicar encuestas de satisfacción y cálculo del porcentaje del indicador.</p> <p>Aplicar y registrar las encuestas de ambiente laboral.</p> <p>Desempeñar todas aquellas actividades que le sean conferidas por la superioridad jerárquica, de acuerdo a la naturaleza, objetivos y atribuciones del área.</p>
	Usuarios:
(Nombre del Usuario *)	Lic. Erika Patricia Quintero Herrera
Cargo*:	Jefa del Departamento de Personal
Funciones*:	<p>Capturar/Imprimir solicitudes, constancias, formatos, notificaciones, contratos y adendas.</p> <p>Aprobar y Firmar electrónicamente los movimientos de personal: alta, baja, promociones, definitividad, art. 51, licencias médicas, sin goce de sueldo menores y mayores a 30 días, licencias sindicales, otros nombramientos, interinatos, defunciones, certificaciones, solicitudes de ropa de trabajo, cambios de talla, revocaciones, retabulaciones, reclasificaciones, cambios de domicilio, entre otros.</p>
Obligaciones*:	Registrar los diversos movimientos que se derivan de la contratación del personal universitario.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Departamento de Personal	
Identificador único*	Sistema Integral de Personal (SIP)
(Nombre del sistema A1*)	Sistema Integral de Personal (SIP)

Tipo de soporte: *	Documentos físicos y Electrónicos
Descripción: *	Expedientes
Características del lugar donde se resguardan los soportes: *	Se resguardan en expedientes laborales por cada trabajador, en orden alfabético por apellido paterno, folder de un color diferente por tipo de personal: amarillo académicos, rojo funcionarios, azul confianza y verde personal de Base, en un archivero horizontal que se encuentra dentro del Archivo del Departamento de Personal que se tiene bajo llave.

### 3. ANÁLISIS DE RIESGOS

Departamento de Personal		
Identificador único*	Sistema Integral de Personal (SIP)	
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP)	
Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado al Departamento de Personal	Medio	Uso de contraseñas seguras cámaras y cerraduras
Fuga de información	Medio	Sólo personal autorizado es el que tiene acceso a la información

### 4. ANÁLISIS DE BRECHA

Departamento de Personal		
Identificador único*	Sistema Integral de Personal (SIP)	
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP)	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*

Identificación y autenticación	Se requiere de un usuario y contraseña para ingresar al sistema y llaves para abrir los muebles	Uso de contraseñas y llaves
Identificación y calificación del personal encargado	Identificar al personal autorizado para realizar trámites en el SIP	Uso de firmas electrónicas sólo de Funcionario

## 5. PLAN DE TRABAJO

Departamento de Personal			
Identificador único*	Sistema Integral de Personal (SIP)		
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP)		
Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Departamento de Personal	
Identificador único*	Sistema Integral de Personal (SIP)
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	La información se escanea y se envía en digital a través del SIP y posteriormente a través de una cita agendada se envía la información soporte en físico a

	través del gestor de la CUAIEED quien ingresa los documentos en la ventanilla de movimientos de personal de la Dirección General de Personal ubicada en Av. Universidad 3000.
Transferencias mediante el traslado de soportes electrónicos:	La información se escanea y se envía en digital a través del SIP.
Transferencias mediante el traslado sobre redes electrónicas:	NA

## II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Se cuenta con cámaras de vigilancia, cerraduras en puertas, así como cerradura en el mueble en el que se resguardan los documentos físicos.

Nombre	Cargo	Funciones	Obligaciones
Lic. Erika Patricia Quintero Herrera	Jefa del Departamento de Personal	Atender, efectuar y registrar los movimientos administrativos del personal adscrito en la Coordinación en materia de derechos, prestaciones y servicios que correspondan, acorde a la normatividad vigente, así como a la Legislación Universitaria y al Sistema de Gestión de la Calidad	<p>Organizar, dirigir y supervisar las actividades del Departamento, desde la elaboración hasta la ejecución de las gestiones.</p> <p>Revisar el cumplimiento de las normas y procedimientos generales de la Institución, así como aplicar las políticas y normas específicas establecidas en el Instituto.</p> <p>Establecer comunicación con instancias internas y externas a la Coordinación, a fin de desarrollar las gestiones propias del Departamento.</p> <p>Verificar que el personal de nuevo ingreso a la dependencia cumpla con los requisitos establecidos por la normatividad aplicable.</p> <p>Atender asuntos que se deriven de la contratación del personal adscrito a la Coordinación.</p> <p>Mantener actualizada la plantilla del personal, conforme a la estructura organizacional de la Institución.</p> <p>Atender y orientar al personal administrativo y académico en asuntos relativos a trámites y procedimientos administrativos.</p> <p>Evaluar el desempeño del personal a su cargo y promover su actualización.</p>

			<p>Organizar la inscripción de los Programas de Estímulos por puntualidad y asistencia, de Calidad y Eficiencia del personal Administrativo de Base y del Programa EDPAC, conforme a las normas establecidas.</p> <p>Emitir el pago de la nómina desde su recepción hasta la devolución.</p> <p>Operar, supervisar y observar que los trámites de los movimientos de altas, bajas y cambios de adscripción del personal de la Entidad se realicen conforme a la normatividad universitaria en vigor, con el propósito de administrar eficazmente la plantilla del personal administrativo de base, confianza, funcionarios y honorarios.</p> <p>Definir, establecer y supervisar los mecanismos internos para el pago oportuno de las remuneraciones y prestaciones a las que tiene derecho el personal (guardería, tiempo extra, Estímulos al Desempeño del Personal Administrativo de Confianza, Programa de Calidad y Eficiencia del Personal de Base, Cláusula 68, Ropa de Trabajo y trámites de prestaciones varias).</p> <p>Colaborar en las actividades de revisión por la dirección específica, de auditorías internas y externas y dar seguimiento a las acciones preventivas, correctivas o de mejora y del servicio no conforme.</p> <p>Participar como Representante del Secretario Administrativo ante el Sistema de Gestión de la Calidad, con las siguientes actividades:</p> <p>Vigilar y asegurar que el personal de cada departamento cumpla las disposiciones de control de documentos del Sistema de Gestión de la Calidad.</p> <p>Identificar las necesidades de recursos y proponer cambios al Sistema de Gestión de la Calidad.</p> <p>Enviar los informes solicitados por la Dirección General de Servicios Administrativos (DGSA).</p> <p>Registrar, controlar, calcular y graficar de la información correspondiente a la medición de los indicadores del Sistema de Gestión de la Calidad de la Coordinación.</p> <p>Coordinar y dar seguimiento a las reuniones de análisis de los resultados y de medición de los indicadores de las auditorías de calidad establecidas por la DGSA.</p> <p>Apoyar la ejecución de las Auditorías de Calidad en la Coordinación</p> <p>Apoyar en el diseño, difusión de materiales y la actualización de formatos del Sistema de Gestión de la Calidad.</p>
--	--	--	--



			<p>Proporcionar a la Secretaría Administrativa los informes de los procesos.</p> <p>Aplicar encuestas de satisfacción y cálculo del porcentaje del indicador.</p> <p>Aplicar y registrar las encuestas de ambiente laboral.</p> <p>Desempeñar todas aquellas actividades que le sean conferidas por la superioridad jerárquica, de acuerdo a la naturaleza, objetivos y atribuciones del área.</p>
--	--	--	--

### III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El servidor lo administra la Dirección de Sistemas de la Dirección General de Personal, toda vez que se trata de un sistema centralizado.

### IV. REGISTRO DE INCIDENTES

La documentación física se encuentra en expedientes por trabajador que se encuentran dentro de un archivero horizontal dentro del Archivo del Departamento de Personal, resguardada bajo llave.

### V. ACCESO A LAS INSTALACIONES

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la Coordinación, para ello se les solicita una identificación oficial vigente y se asigna un gafete. La Coordinación se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el director de la Dirección de Desarrollo de Sistemas para la Educación de la CUAIEED.

### VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La Dirección de Sistemas de la Dirección General de Personal funge como desarrollador y administrador del SIP, el Departamento de Personal de la CUAIEED sólo es usuario del mismo.

### VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los roles de usuario que maneja el SIP son establecidos y otorgados por la Dirección de Sistemas de la Dirección General de Personal.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

La Dirección de Sistemas de la Dirección General de Personal es la responsable de respaldar y recuperar datos del SIP.

## IX. PLAN DE CONTINGENCIA

La Dirección de Sistemas de la Dirección General de Personal es la responsable de desarrollar un plan de contingencia del SIP para asegurar la integridad de la información almacenada en dicho sistema.

### 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

#### 7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Departamento de Personal		
Identificador único*	Sistema Integral de Personal (SIP)	
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP)	
Recurso*	Descripción*	Control*
No aplica	No aplica	No aplica

#### 7.2 Procedimiento para la revisión de las medidas de seguridad

Departamento de Personal		
Identificador único*	Sistema Integral de Personal (SIP)	
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP)	
Medida de seguridad*	Procedimiento*	Responsable*
No aplica	No aplica.	Dirección General de Proveduría

#### 7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Departamento de Personal		
Identificador único*	Sistema Integral de Personal (SIP)	
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP)	
Medida de seguridad*	Resultado de evaluación*	Responsable*
No aplica	No aplica	Dirección General de Proveduría

#### 7.4 Acciones para la corrección y actualización de las medidas de seguridad

Departamento de Personal		
Identificador único*	Sistema Integral de Personal (SIP)	
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP)	
Medida de seguridad*	Acciones*	Responsable*
No aplica	No aplica	Dirección General de Proveduría

### 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

#### 8.1 Programa de capacitación a los responsables de seguridad de datos personales

La Dirección General de Personal es la responsable de impartir las capacitaciones del sistema.

#### 8.2 Programa de difusión de la protección a los datos personales

No se tiene un programa de difusión de la protección a los datos personales

### 9. MEJORA CONTINUA

#### 9.1 Actualización y mantenimiento de sistemas de información

Departamento de Personal			
Identificador único*	Sistema Integral de Personal (SIP)		
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP)		
Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

## 9.2 Actualización y mantenimiento de equipo de cómputo

Departamento de Personal			
Identificador único*	Sistema Integral de Personal (SIP)		
(Nombre del sistema A1*:	Sistema Integral de Personal (SIP)		
Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

## 9.3 Procesos para la conservación, preservación y respaldos de información

Departamento de Personal		
Identificador único*	Sistema Integral de Personal (SIP)	
(Nombre del sistema A1*:	Sistema Integral de Personal (SIP)	
Proceso*	Descripción*	Responsable*
No aplica	No aplica	Dirección General de Proveeduría

## 9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Departamento de Personal		
Identificador único*	Sistema Integral de Personal (SIP)	
(Nombre del sistema A1*:	Sistema Integral de Personal (SIP)	
Proceso*	Descripción*	Responsable*
No aplica	No aplica	Dirección General de Proveeduría

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No aplica

### **Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios.**

#### **Introducción**

El Sistema Integral de Personal es un sistema centralizado y desarrollado por la Dirección de Sistemas de la Dirección General de Personal de la UNAM, a través del cual los diferentes Departamentos de Personal de la UNAM incluyendo el de la CUAIEED, operamos los siguientes trámites:

- Contratación de personal
- Trámite de licencias médicas, sin sueldo menores y mayores a 30 días, licencias sindicales.
- Movimientos de personal: Altas, Bajas, Otros nombramientos, Renuncias, Defunciones, Cambios de horario, Definitividad, Art. 51 del EPA, interinatos, laudos, permutas, reanudación de labores, reinstalaciones, reclasificaciones, retabulaciones, revocaciones, término de nombramientos,
- Promoción personal administrativo de Base
- Oficio Certificación / Diferimiento para Personal Académico
- Solicitud Programa de Retiro por Jubilación / Pensión
- Solicitud de Certificación Jubilación / Pensión
- Oficio de Solicitud de Cobertura de plaza personal administrativo de Base
- Designación de Beneficiarios para Pago de Marcha
- Solicitud de Pago de Ayuda de Guardería
- Solicitud de Cambio de Domicilio
- Solicitud de Credencial
- Ropa de Trabajo
- Autorización de Contratos y Adendas
- Autorización de Notificaciones
- Constancias de Empleo y Sueldo
- Seguimiento Relaciones DGAPA

- Generación de Carta de Confidencialidad

## 1. INVENTARIO DE TRATAMIENTO DE DATOS PERSONALES

Departamento de Personal- Contratación de Servicios Profesionales	
Identificador único*	UNAM:4C.14/482-2022
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios.
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de identificación: Nombre, domicilio, teléfono, correo electrónico, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, y nacionalidad. Datos académicos: Títulos y Cédula Profesional Datos laborales: Cargo, actividades e importes de pago
Responsable*:	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
Nombre*:	Lic. Erika Patricia Quintero Herrera
Cargo*:	Jefa del Departamento de Personal
Funciones*:	Vigilar el cumplimiento de la atención de solicitudes realizadas por las áreas sustantivas de la Dependencia. Dando inicio y registro a los trámites en el SIP, así como la culminación y cierre de los mismos.
Obligaciones*:	Revisar la atención de Solicitudes de Contratación Validar que todos los trámites cuenten con la información correcta de los prestadores de servicios. Validar el registro de los prestadores de Servicios en el SIP. Verificar el cierre de los trámites en el SIP con la información obtenida a lo largo el proceso.
	Encargados:
(Nombre del Encargado 1*)	Lic. Lilia Paola Arredondo González
Cargo*:	Jefa de Área de Contratación de Servicios Profesionales
Funciones*:	Revisar y atender las solicitudes de contratación en apego con lo dispuesto en las norma y políticas de la Institución. Revisar la documentación presentada por el área sustantiva
Obligaciones*:	Atender en el marco normativo toda solicitud de contratación de servicios profesionales.

	<p>Revisar que el área sustantiva presente la documentación completa y necesaria para la contratación de servicios profesionales.</p> <p>Resguardar las solicitudes de contratación con la información correspondiente.</p> <p>Revisar que la documentación enviada por las áreas sustantivas con respecto a los prestadores de servicios cumpla con los lineamientos</p> <p>Asistir al proceso de envío y devolución de certificación de contratos por medio del Sistema ante la Dirección General de Personal.</p>
	Usuarios:
(Nombre del Encargado 2 *)	Lic. Héctor Alejandro Mancera González
Cargo*:	Asistente de Procesos
Funciones*:	Asistir al proceso de contratación de servicios Profesionales.
Obligaciones*:	<p>Revisar que la documentación enviada por las áreas sustantivas con respecto a los prestadores de servicios cumpla con los lineamientos</p> <p>Asistir al proceso de envío y devolución de certificación de contratos por medio del Sistema ante la Dirección General de Personal.</p>

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Departamento de Personal- Contratación de Servicios Profesionales	
Identificador único*	UNAM:4C.14/482-2022
(Nombre del sistema A1*)	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios.
Tipo de soporte: *	Electrónico y documentos físicos
Descripción: *	Expedientes y base de datos
Características del lugar donde se resguardan los soportes: *	Se resguardan las carpetas en el Departamento de Personal y en una oficina particular que cuenta con llave y en electrónico en la computadora de la jefa del Área de Contratación de Servicios Profesionales y el asistente de procesos, ambas computadoras cuentan con contraseñas que solo conocen los usuarios de ellas. Adicionalmente el sistema requiere usuario y

contraseña la cual es otorgada a través del área de sistemas de la DGPe, la cual solo los usuarios conocen

### 3. ANÁLISIS DE RIESGOS

Departamento de Personal- Contratación de Servicios Profesionales		
Identificador único*	UNAM:4C.14/482-2022	
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios.	
Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado a la oficina del Área de Contratación de Servicios profesionales	Medio	Uso de contraseñas seguras cámaras y cerraduras
Fuga de información	Medio	Sólo personal autorizado es el que tiene acceso a la información

### 4. ANÁLISIS DE BRECHA

Departamento de Personal- Contratación de Servicios Profesionales		
Identificador único*	UNAM:4C.14/482-2022	
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios.	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Identificación y autenticación	Se requiere de un usuario y contraseña para ingresar al sistema y llaves para abrir los muebles	Uso de contraseñas y llaves

### 5. PLAN DE TRABAJO



Departamento de Personal- Contratación de Servicios Profesionales			
Identificador único*	UNAM:4C.14/482-2022		
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios		
Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Departamento de Personal- Contratación de Servicios Profesionales	
Identificador único*	UNAM:4C.14/482-2022
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios.
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	La entrega de las solicitudes de contratación se realiza por medio de oficio por parte de las áreas sustantivas de la dependencia directamente a la Secretaria Administrativa y se acusa de entrega.
Transferencias mediante el traslado de soportes electrónicos:	La transferencia de la información de los prestadores de servicios se hace mediante una carpeta compartida con los enlaces de las áreas, el acceso a las computadoras que tienen esta información cuenta con claves.
Transferencias mediante el traslado sobre redes electrónicas:	Se utiliza red privada en la CUAIEED

## II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Se cuenta con cámaras de vigilancia y cerraduras en puertas.

Nombre	Cargo	Funciones	Obligaciones
Lic. Lilia Paola Arredondo González	Jefa del Departamento de Bienes y Suministros	Revisar y atender las solicitudes de contratación en apego con lo dispuesto en las norma y políticas de la Institución.  Revisar la documentación presentada por el área sustantiva	Atender en el marco normativo toda solicitud de contratación de servicios profesionales. Revisar que el área sustantiva presente la documentación completa y necesaria para la contratación de servicios profesionales. Resguardar las solicitudes de contratación con la información correspondiente. Revisar que la documentación enviada por las áreas sustantivas con respecto a los prestadores de servicios cumpla con los lineamientos

## III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No podemos tener un control debido a que nosotros no somos responsables de administrar el servidor.

## IV. REGISTRO DE INCIDENTES

Sobre el registro electrónico no podemos tener control en caso de que exista un incidente, sin embargo, en el registro en físico se mantiene la documentación bajo llave.

## V. ACCESO A LAS INSTALACIONES

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente y se asigna un gafete. La dependencia se encuentra resguardada en

todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el director de la Dirección de Desarrollo de Sistemas para la Educación.

## VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Nosotros no tenemos los permisos para agregar o quitar datos personales de ninguno de los usuarios registrados en el SIP.

## VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los accesos al sistema SIP, lo establece la Dirección General de Personal.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

La Dirección General de Personal es la encargada de respaldar y recuperar datos del SIP.

## IX. PLAN DE CONTINGENCIA

La Dirección General de Personal es la responsable de desarrollar un plan de contingencia del SIP.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Departamento de Personal- Contratación de Servicios Profesionales		
Identificador único*	UNAM-4C-14/482-2022	
(Nombre del sistema A1)*	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios	
Recurso*	Descripción*	Control*
No aplica	No aplica	No aplica

### 7.2 Procedimiento para la revisión de las medidas de seguridad

Departamento de Personal- Contratación de Servicios Profesionales		
Identificador único*	UNAM:4C.14/482-2022	
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios	
Medida de seguridad*	Procedimiento*	Responsable*
No aplica	No aplica.	Dirección General de Proveduría

### 7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Departamento de Personal- Contratación de Servicios Profesionales		
Identificador único*	UNAM:4C.14/482-2022	
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios	
Medida de seguridad*	Resultado de evaluación*	Responsable*
No aplica	No aplica	Dirección General de Proveduría

### 7.4 Acciones para la corrección y actualización de las medidas de seguridad

Departamento de Personal- Contratación de Servicios Profesionales		
Identificador único*	UNAM:4C.14/482-2022	
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios	
Medida de seguridad*	Acciones*	Responsable*
No aplica	No aplica	Dirección General de Proveduría

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

## 8.1 Programa de capacitación a los responsables de seguridad de datos personales

La Dirección General de Personal es la encargada de impartir las capacitaciones del sistema

## 8.2 Programa de difusión de la protección a los datos personales

No se tiene un programa de difusión de la protección a los datos personales

## 9. MEJORA CONTINUA

### 9.1 Actualización y mantenimiento de sistemas de información

Departamento de Personal- Contratación de Servicios Profesionales			
Identificador único*	UNAM:4C.14/482-2022		
(Nombre del sistema A1) *	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios.		
Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

### 9.2 Actualización y mantenimiento de equipo de cómputo

Departamento de Personal- Contratación de Servicios Profesionales			
Identificador único*	UNAM:4C.14/482-2022		
(Nombre del sistema A1*:	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios.		
Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

### 9.3 Procesos para la conservación, preservación y respaldos de información

Departamento de Personal- Contratación de Servicios Profesionales		
Identificador único*	UNAM:4C.14/482-2022	
(Nombre del sistema A1*:	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios.	
Proceso*	Descripción*	Responsable*
No aplica	No aplica	Dirección General de Proveduría

#### 9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Departamento de Personal- Contratación de Servicios Profesionales		
Identificador único*	UNAM:4C.14/482-2022	
(Nombre del sistema A1*:	Sistema Integral de Personal (SIP) Módulo de Prestación de Servicios.	
Proceso*	Descripción*	Responsable*
No aplica	No aplica	Dirección General de Proveduría

#### 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No aplica

#### **Sistema Integral de Administración Financiera**

##### **Introducción**

Hoy en día es muy importante la adquisición de información veraz y oportuna, la tecnología nos ayuda a hacer esto posible. Pero más aún se requiere de personas con visión para aplicar esta tecnología en áreas específicas. Este ha sido el caso de la M. en I. Rosalía Aldana, quien se ha involucrado con las personas quienes realizan estas tareas, esto le ha permitido en primer lugar hablar su "lenguaje" con lo cual la comunicación se establece y por otra la actitud profesional que siempre ha demostrado. A la par de tener el conocimiento tecnológico y haberse "ensuciado las manos", es decir, aprendiendo las diversas tareas del área administrativa.

Ya en la segunda mitad de los años 80, se inicia un proceso evolutivo en el área administrativa del Instituto de Ingeniería de la UNAM, al dar apoyo realizando pequeños programas para la automatización de esta área, con la colaboración de cierto personal quienes desde un principio demostraron su entusiasmo a la perspectiva de una reforma en la forma de llevar a cabo su trabajo. Más aún en algunas otras dependencias que tuvieron a bien integrar estos módulos en su área administrativa al comprobar las bondades que estos les proporcionaban se enriqueció el conocimiento del funcionamiento de la UNAM en la forma de trámite y elaboración de la información.

La idea original del S.I.A.F. surge a partir de la necesidad de automatizar los procesos relacionados con el área administrativa y cumpliendo con los requerimientos de llevar una contabilidad integral estipulado para todas las dependencias. Con la experiencia acumulada que se tuvo con los módulos anteriores elaborados con "Clipper", y ahora tomando como herramienta Visual FoxPro para su desarrollo. Los módulos se interrelacionan, comparten su información, por lo que es muy conveniente el trabajarlos conjuntamente, aunque se pueden trabajar por separado tan solo realizando alguna pequeña intervención inicial en tablas específicas. De lo anterior se sigue que estos módulos trabajan en ambiente multiusuario (en Red) lo que permite apreciar las modificaciones casi enseguida.

## 1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Departamento de Presupuesto	
Identificador único*	Apl_482 (//172.16.3.150) (z)
Nombre del sistema A1*:	Sistema Integral de Administración Financiera
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de proveedores, montos pagados, firmas de responsables, facturas
Responsable*:	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).
Nombre*:	L.C. Erick Arturo Hernández Moreno
Cargo*:	Jefa del Departamento de Presupuesto
Funciones*:	Registros contables de los gastos realizados mensualmente en la Dependencia y registro de partidas y cuentas provenientes del gasto. Conciliaciones mensuales de los registros en el Sistema vs los registros de la UNAM
Obligaciones*:	Generar conciliaciones ante la Dirección General de Finanzas Contar con los estados financieros mensuales Realizar cortes mensuales

	Usuarios:
(Nombre del Usuario *)	Jefe de Departamento de Presupuesto y colaboradores a quienes previamente se les conceden permisos
Cargo*:	Funcionarios, Académicos y Confianza
Funciones*:	Capturar gastos Ejecutar conciliaciones
Obligaciones*:	Dar seguimiento al ejercicio de los ingresos extraordinarios de la CUAIEED.  Registrar transferencias de los ingresos y gastos de las cuentas de ingresos extraordinarios.  Realizar conciliaciones de los ingresos extraordinarios.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Departamento de Presupuesto	
Identificador único*	Apl_482 (//172.16.3.150) (z)
(Nombre del sistema A1*)	Sistema Integral de Administración Financiera
Tipo de soporte: *	Electrónico y documentos físicos
Descripción: *	Expedientes y base de datos
Características del lugar donde se resguardan los soportes: *	Se resguardan las carpetas en el Departamento de Presupuesto en un mueble que cuenta con llave y en electrónico en la computadora del jefe del Departamento, la cual tiene contraseña

## 3. ANÁLISIS DE RIESGOS

Departamento de Presupuesto	
Identificador único*	Apl_482 (//172.16.3.150) (z)
(Nombre del sistema A1*)	Sistema Integral de Administración Financiera



Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado al Departamento de Presupuesto	Medio	Uso de contraseñas seguras, cámaras y cerraduras
Fuga de información	Medio	Sólo personal autorizado es el que tiene acceso a la información

#### 4. ANÁLISIS DE BRECHA

Departamento de Presupuesto		
Identificador único*	Apl. 482 (//172.16.3.150) (z)	
(Nombre del sistema A1) *	Sistema Integral de Administración Financiera	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Identificación y autenticación	Se requiere de un usuario y contraseña para ingresar al sistema y llaves para abrir los muebles	Uso de contraseñas y llaves
Identificación y calificación del personal encargado	Identificar al personal autorizado para realizar trámites en el SIAF	Uso de firmas electrónicas sólo de Funcionarios

#### 5. PLAN DE TRABAJO

Departamento de Presupuesto			
Identificador único*	Apl. 482 (//172.16.3.150) (z)		
(Nombre del sistema A1) *	Sistema Integral de Administración Financiera		
Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Departamento de Presupuesto	
Identificador único*	Apl_482 (//172.16.3.150) (z)
(Nombre del sistema A1) *	Sistema Integral de Administración Financiera
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	La comunicación con el usuario se realiza vía correo electrónico
Transferencias mediante el traslado de soportes electrónicos:	La comunicación con dependencias centrales se realiza vía correo electrónico
Transferencias mediante el traslado sobre redes electrónicas:	Se utiliza red privada en la CUAIEED

### II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Se cuenta con cámaras de vigilancia, cerraduras en puertas, así como cerradura en el mueble en el que se resguardan los documentos físicos.

Nombre	Cargo	Funciones	Obligaciones
L.C. Erick Arturo Hernández Moreno	Jefa del Departamento de Presupuesto	Registro y control del presupuesto asignado. Análisis y evaluación del ejercicio presupuestal institucional y reprogramación de la asignación de recursos. Efectuar análisis de los gastos realizados con recursos del fondo fijo para realizar su pronto reembolso. Trámite de pago a proveedores por compra de	Registro contable de ingresos y gastos de forma mensual Generar pólizas correspondientes a transferencias, pagos y ejercicio del gasto Generar conciliaciones en el sistema y bancarias manualmente.

		bienes o prestaciones de servicios. Gestión y trámite del pago de honorarios por servicios profesionales. Manejo de Cuentas por Cobrar para su correcta depuración y conciliación.	
--	--	--	--

### III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No podemos tener un control debido a que nosotros no somos responsables de administrar el servidor.

### IV. REGISTRO DE INCIDENTES

Sobre el registro electrónico no podemos tener control en caso de que exista un incidente, sin embargo, en el registro incidentes físicos, se mantiene la documentación bajo llave.

### V. ACCESO A LAS INSTALACIONES

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente y se asigna un gafete. La dependencia se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el director de la Dirección de Desarrollo de Sistemas para la Educación.

### VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Nosotros no tenemos los permisos para agregar o quitar datos personales de ninguno de los usuarios registrados en el SIAF.

### VII. PERFILES DE USUARIO Y CONTRASEÑAS

Los roles del usuario que se manejan en el SIAF son establecidos por los desarrolladores del mismo, el jefe del Depto. da de alta a los nuevos usuarios, con base en lo que indique el responsable de cada área.

## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El Instituto de Ingeniería es el encargado de respaldar y recuperar datos del SIAF.

## IX. PLAN DE CONTINGENCIA

El Instituto de Ingeniería es el encargado.

## 7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

### 7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Departamento de Presupuesto		
Identificador único*	Apl_482 (//172.16.3.150) (z)	
(Nombre del sistema A1) *	Sistema Integral de Administración Financiera	
Recurso*	Descripción*	Control*
No aplica	No aplica	No aplica

### 7.2 Procedimiento para la revisión de las medidas de seguridad

Departamento de Presupuesto		
Identificador único*	Apl_482 (//172.16.3.150) (z)	
(Nombre del sistema A1) *	Sistema Integral de Administración Financiera	
Medida de seguridad*	Procedimiento*	Responsable*
No aplica	No aplica.	Instituto de Ingeniería

### 7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Departamento de Presupuesto	
Identificador único*	Apl_482 (//172.16.3.150) (z)
(Nombre del sistema A1) *	Sistema Integral de Administración Financiera

Medida de seguridad*	Resultado de evaluación*	Responsable*
No aplica	No aplica	Instituto de Ingeniería

#### 7.4 Acciones para la corrección y actualización de las medidas de seguridad

Departamento de Presupuesto		
Identificador único*	Apl_482 (//172.16.3.150) (z)	
(Nombre del sistema A1) *	Sistema Integral de Administración Financiera	
Medida de seguridad*	Acciones*	Responsable*
No aplica	No aplica	Instituto de Ingeniería

### 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

#### 8.1 Programa de capacitación a los responsables de seguridad de datos personales

La Dirección General de Proveduría es la encargada de impartir las capacitaciones del sistema

#### 8.2 Programa de difusión de la protección a los datos personales

No se tiene un programa de difusión de la protección a los datos personales

### 9. MEJORA CONTINUA

#### 9.1 Actualización y mantenimiento de sistemas de información

Departamento de Presupuesto			
Identificador único*	Apl_482 (//172.16.3.150) (z)		
(Nombre del sistema A1) *	Sistema Integral de Administración Financiera		
Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

## 9.2 Actualización y mantenimiento de equipo de cómputo

Departamento de Presupuesto			
Identificador único*	Apl_482 (//172.16.3.150) (z)		
(Nombre del sistema A1*:	Sistema Integral de Administración Financiera		
Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

## 9.3 Procesos para la conservación, preservación y respaldos de información

Departamento de Presupuesto		
Identificador único*	Apl_482 (//172.16.3.150) (z)	
(Nombre del sistema A1*:	Sistema Integral de Administración Financiera	
Proceso*	Descripción*	Responsable*
No aplica	No aplica	Instituto de Ingeniería

## 9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Departamento de Presupuesto		
Identificador único*	Apl_482 (//172.16.3.150) (z)	
(Nombre del sistema A1*:	Sistema Integral de Administración Financiera	
Proceso*	Descripción*	Responsable*
No aplica	No aplica	Instituto de Ingeniería

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No aplica

## **Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)**

### **Introducción**

En cumplimiento a lo dispuesto en los puntos 3 y 5 de las Políticas en materia de obra y servicios relacionados con la misma, los cuales establecen que las dependencias y entidades universitarias podrán llevar a cabo obras y servicios, previo dictamen, verificación y aprobación de la Dirección General de Obras y Conservación; con base en el ACUERDO CINCO, emitido por el Comité Asesor de Obras, en su Tercera Sesión Ordinaria, celebrada el 11 de agosto de 2011, mediante el cual aprobó la creación del Programa de aprobación y seguimiento a asignaciones de obra y servicios relacionados con la misma y en términos de lo dispuesto en la Circular publicada en la Gaceta UNAM el 20 de febrero de 2012, sobre dicho programa, se les solicita incorporar y registrar información sobre las obras y servicios que pretenden ejecutar correspondientes al ejercicio del año en curso.

### **Beneficios**

Proporcionar una herramienta administrativa enfocada a apoyar:

- Una adecuada coordinación en el desarrollo de las obras y servicios que se realicen en la infraestructura universitaria.
- Garantizar la correcta aplicación de la Normatividad de Obras
- Dar transparencia al manejo de los recursos de la UNAM.
- Al utilizar un sistema de gestión y la firma electrónica avanzada como un mecanismo de seguridad y simplificación de las autorizaciones se disminuye de manera considerable el uso excesivo de papel en los trámites.

## **1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES**

Superintendencia de Obras	
Identificador único*	UNAM:7C.1/482
Nombre del sistema A1*:	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)
Datos personales (sensibles o no) contenidos en el sistema*:	Nombres y currículum vitae del personal responsable para dirigir el trabajo. Nombre y registro de proveedor ante la DGOyC
Responsable*:	Coordinación de Universidad Abierta, Innovación Educativa, y Educación a Distancia (CUAIEED).

Nombre*:	Erick Alonso Granados Garnica
Cargo*:	Superintendente de obra
Funciones*:	Vigilar la ejecución de los trabajos en materia de rehabilitación, ampliación, remodelación y servicios relacionados con la obra
Obligaciones*:	Registrar los proyectos de rehabilitación, ampliación, remodelación y servicios relacionados con la obra.  Cotizar, generar cuadros comparativos y estudios de mercado de los trabajos solicitados y realizar el concurso correspondiente.  Solicitar el dictamen de validación aprobatorio para realizar los trabajos.
	Usuarios:
(Nombre del Usuario *)	Erick Alonso Granados Garnica
Cargo*:	Funcionario
Funciones*:	Capturar/Registrar la obra a realizar Solicitar la validación de la obra. Realizar el cierre de obra en sistema.
Obligaciones*:	Registrar la obra a realizar, subir la información correspondiente a los trabajos y cerrar la obra en el sistema.

## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Departamento Superintendencia de Obras	
Identificador único*	UNAM:7C.1/482
(Nombre del sistema A1*)	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)
Tipo de soporte: *	Electrónico y documentos físicos
Descripción: *	Expedientes y base de datos



Características del lugar donde se resguardan los soportes: *	Se resguardan las carpetas en la Superintendencia de Obra en closet con llave y en electrónico en la nube
---	---

### 3. ANÁLISIS DE RIESGOS

Superintendencia de Obras		
Identificador único*	UNAM:7C.1/482	
(Nombre del sistema A1) *	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)	
Riesgo*	Impacto*	Mitigación*
Ingreso no autorizado a la Superintendencia de Obras	Medio	Uso de contraseñas seguras cámaras y cerraduras
Fuga de información	Medio	Sólo personal autorizado es el que tiene acceso a la información

### 4. ANÁLISIS DE BRECHA

Superintendencia de Obras		
Identificador único*	UNAM:7C.1/482	
(Nombre del sistema A1) *	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
Identificación y autenticación	Se requiere de un usuario y contraseña para ingresar al sistema y llaves para abrir los muebles	Uso de contraseñas y llaves

Identificación y calificación del personal encargado	Identificar al personal autorizado para realizar trámites en el PASAOR	Uso de contraseñas solo por funcionarios
--	--	--

## 5. PLAN DE TRABAJO

Superintendencia de Obras			
Identificador único*	UNAM:7C.1/482		
(Nombre del sistema A1) *	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)		
Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

Superintendencia de Obras	
Identificador único*	UNAM:7C.1/482
(Nombre del sistema A1) *	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	El envío de la información se realiza a través del sistema
Transferencias mediante el traslado de soportes electrónicos:	El envío de la información se realiza a través del sistema.
Transferencias mediante el traslado sobre redes electrónicas:	Se utiliza red privada en la CUAIEED

## V. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Se cuenta con cámaras de vigilancia, cerraduras en puertas, así como cerradura en el mueble en el que se resguardan los documentos físicos.

Nombre	Cargo	Funciones	Obligaciones
Arq, Erick Alonso Granados Garnica	Superintendente de Obra	Vigilar el proceso de registro correcto de los trabajos de obra o servicios relacionados con la misma, así como su correcta ejecución por parte del proveedor asignado, de acuerdo a la Normatividad en Materia de Obras y servicios relacionados con la misma.	Establecer el programa de trabajo de acuerdo a las necesidades del espacio de acuerdo a la normatividad vigente. Cotizar, generar cuadros comparativos y estudios de mercado y realizar el concurso correspondiente. Registrar documentación y datos de los trabajos a realizar. Solicitar validación de dictamen.

## VI. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No podemos tener un control debido a que nosotros no somos responsables de administrar el servidor.

## VII. REGISTRO DE INCIDENTES

Sobre el registro electrónico no podemos tener control en caso de que exista un incidente, sin embargo, sobre el registro físico, se mantiene la documentación bajo llave.

## V. ACCESO A LAS INSTALACIONES

La seguridad perimetral exterior se encuentra resguardada por el personal de vigilancia de la CUAIEED todo el año con un servicio 24/7. Se cuenta con una caseta de vigilancia que registra los accesos de todas las personas que ingresan a la dependencia, para ello se les solicita una identificación oficial vigente y se asigna un gafete. La dependencia se encuentra resguardada en todo su perímetro por cercas coronadas con alambres de púas. Adicionalmente se cuenta con un

sistema de videovigilancia que funciona las veinticuatro horas del día coordinado con las autoridades universitarias.

La seguridad perimetral interior que resguarda los sistemas electrónicos se encuentra dentro de un centro de datos ubicado al interior de la Coordinación. El acceso se controla mediante el uso de biométricos (huella dactilar). El sistema toma una fotografía, hora y fecha de todo intento de ingreso (exitoso y fallido). El acceso al centro de datos se otorga mediante una autorización emitida por el director de la Dirección de Desarrollo de Sistemas para la Educación.

## **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**

Nosotros no tenemos los permisos para agregar o quitar datos personales de ninguno de los usuarios registrados en el PASAOR.

## **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

El usuario y contraseña para acceder es el asignado en el Sistema de Autenticación para Aplicaciones de la Secretaría Administrativa de la UNAM y el alta del funcionario responsable por la Secretaría Administrativa de la Dependencia.

## **VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS**

La Dirección General de Obras y Conservación es la encargada de respaldar y recuperar datos del PASAOR.

## **IX. PLAN DE CONTINGENCIA**

La Dirección General de Obras y Conservación es la responsable de desarrollar un plan de contingencia del PASAOR.

## **7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD**

### **7.1 Herramientas y recursos para monitoreo de la protección de datos personales**

Superintendencia de Obras		
Identificador único*	UNAM:7C.1/482	
(Nombre del sistema A1) *	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)	
Recurso*	Descripción*	Control*
No aplica	No aplica	No aplica

## 7.2 Procedimiento para la revisión de las medidas de seguridad

Superintendencia de Obras		
Identificador único*	UNAM:7C.1/482	
(Nombre del sistema A1) *	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)	
Medida de seguridad*	Procedimiento*	Responsable*
No aplica	No aplica.	Dirección General de Obras y Conservación

## 7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Superintendencia de Obras		
Identificador único*	UNAM:7C.1/482	
(Nombre del sistema A1) *	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)	
Medida de seguridad*	Resultado de evaluación*	Responsable*
No aplica	No aplica	Dirección General de Obras y Conservación General de Proveduría

## 7.4 Acciones para la corrección y actualización de las medidas de seguridad

Superintendencia de Obras	
Identificador único*	UNAM:7C.1/482
(Nombre del sistema A1) *	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)

Medida de seguridad*	Acciones*	Responsable*
No aplica	No aplica	Dirección General de Obras y Conservación

## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

### 8.1 Programa de capacitación a los responsables de seguridad de datos personales

La Dirección General de Obras y Conservación es la encargada de impartir las capacitaciones del sistema

### 8.2 Programa de difusión de la protección a los datos personales

No se tiene un programa de difusión de la protección a los datos personales

## 9. MEJORA CONTINUA

### 9.1 Actualización y mantenimiento de sistemas de información

Superintendencia de Obras			
Identificador único*	UNAM:7C.1/482		
(Nombre del sistema A1) *	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)		
Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

### 9.2 Actualización y mantenimiento de equipo de cómputo

Superintendencia de Obras	
Identificador único*	UNAM:7C.1/482
(Nombre del sistema A1*:	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)

Actividad*	Descripción*	Duración*	Cobertura*
No aplica	No aplica	No aplica	No aplica

### 9.3 Procesos para la conservación, preservación y respaldos de información

Superintendencia de Obras		
Identificador único*	UNAM:7C.1/482	
(Nombre del sistema A1*:	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)	
Proceso*	Descripción*	Responsable*
No aplica	No aplica	Dirección General de Obras y Conservación

### 9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos



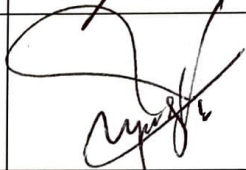
Superintendencia de Obras		
Identificador único*	UNAM:7C.1/482	
(Nombre del sistema A1*:	Programa de Aprobación y Seguimiento a Asignaciones de Obra y Servicios Relacionados con la misma (PASAOR)	
Proceso*	Descripción*	Responsable*
No aplica	No aplica	Dirección General de Obras y Conservación

## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No aplica

## Aprobación del documento de seguridad

Formato con firmas que acreditan la confidencialidad del documento

		Nombre y firma de quienes revisaron el presente documento
<b>Responsable del desarrollo</b>	Ing. Milton Arturo García Lima Jefe de la Unidad Sistemas para la Evaluación Educativa Tel. oficina 55-56221509 <a href="mailto:milton_garcia@cuaieed.unam.mx">milton_garcia@cuaieed.unam.mx</a>	
<b>Revisó</b>	Mtro. Ricardo Arroyo Mendoza Director de Desarrollo de Sistemas para la Educación Tel. oficina 55-56228744 <a href="mailto:ricardo_arroyo@cuaieed.unam.mx">ricardo_arroyo@cuaieed.unam.mx</a>	
<b>Autorizó</b>	Dr. Melchor Sánchez Mendiola Coordinador Tel. oficina 55-56226666 <a href="mailto:melchor_sanchez@cuaieed.unam.mx">melchor_sanchez@cuaieed.unam.mx</a>	
<b>Fecha de aprobación</b>		27/09/2022
<b>Fecha de actualización</b>		27/09/2022



## **FUNDAMENTO LEGAL QUE SUSTENTA LA RESERVA, ASÍ COMO EL PLAZO DE ÉSTA.**

*“Por lo antes mencionado, se colman las hipótesis de las fracciones I, II y III, dispuestas en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, por lo que es procedente **CONFIRMAR** la reserva total de una parte de la información para la elaboración de la versión pública propuesta por la Coordinación de Universidad Abierta, Innovación Educativa y Educación a Distancia (**CUAIEED**), por un periodo de cinco años, de conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.”*