DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES DE LA FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

El presente documento de seguridad contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales de la Facultad de Contaduría y Administración (FCA) con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Enero 2024.

ÍNDICE

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 la Facultad de Contaduría y Administración de la UNAM, 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 describan 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 encuentra 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".*

INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

A1 SISTEMA DE INVENTARIOS FCA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASI01
(Nombre del sistema A1)	Sistema de inventarios FCA
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre de los responsables para uso de un bien de la Facultad (académicos de tiempo completo y personal administrativo)
Responsable:	
Nombre*:	**Balfred Santaella Hinojosa**
Cargo*:	**Jefe del Centro de Informática**
Funciones*:	Planeación, organización y control de los sistemas de información de la Facultad.
Obligaciones*:	Asegurar el funcionamiento de los sistemas y servicios de información.
	Encargados:
(Nombre del Encargado 1*)	**Raúl Esteban Cruz Quiroz**
Cargo*:	**Responsable de Infraestructura**
Funciones*:	Soporte en la base de datos de nombre y apellidos de los académicos de tiempo completo y personal administrativo adscrito a la FCA para poder establecer un vínculo con los bienes a su cargo.
Obligaciones*:	Validar y mantener la confidencialidad de los datos personales (nombre y apellidos) para uso exclusivo de la elaboración de resguardos de bienes. Asegurar la integridad de la información de datos personales registrada en la base de datos del sistema.
	Usuarios:
(Nombre del Usuario 1)	Pablo Solís Tapia
Cargo*:	Jefe de Inventarios de la Secretaría Administrativa
Funciones*:	Utilizar únicamente el nombre de un académico de tiempo completo o personal administrativo para establecer la relación de bienes de pertenecientes a la Facultad, los cuales deberá resguardar el usuario que los recibe para el desempeño de sus funciones.
Obligaciones*:	Mantener la confidencialidad de los datos personales (nombre y apellidos) para uso exclusivo de la elaboración de resguardos de bienes.

	Resguardar el documento físico F01-GO-BS 0301 Revisión 00 (Resguardo de bienes inventariables) que contiene nombre y firma de conformidad del usuario y de quien da su visto bueno.

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

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único:	FCASI01
(Nombre del sistema A1)	Sistema de inventarios FCA
Tipo de soporte:	Soporte físico y electrónico.
Descripción:	Soporte físico: formato F01-GO-BS 0301 Revisión 00 (Resguardo de bienes inventariables) Soporte electrónico: base de datos relacional
Características del lugar donde se resguardan los soportes:	Soporte físico: oficina con ventilación natural, luz natural y artificial, puerta de acceso de madera y chapa, aislada de humedad, con archiveros y libreros que permiten la conservación adecuada de los documentos. Soporte electrónico: base de datos relacional en un servidor ubicado en el Centro de Informática de la FCA

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASI01	
(Nombre del sistema A1)	Sistema de inventarios FCA	
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]

[1] **Texto eliminado:** Apartado correspondiente a “Análisis de Riesgos” (página 4). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

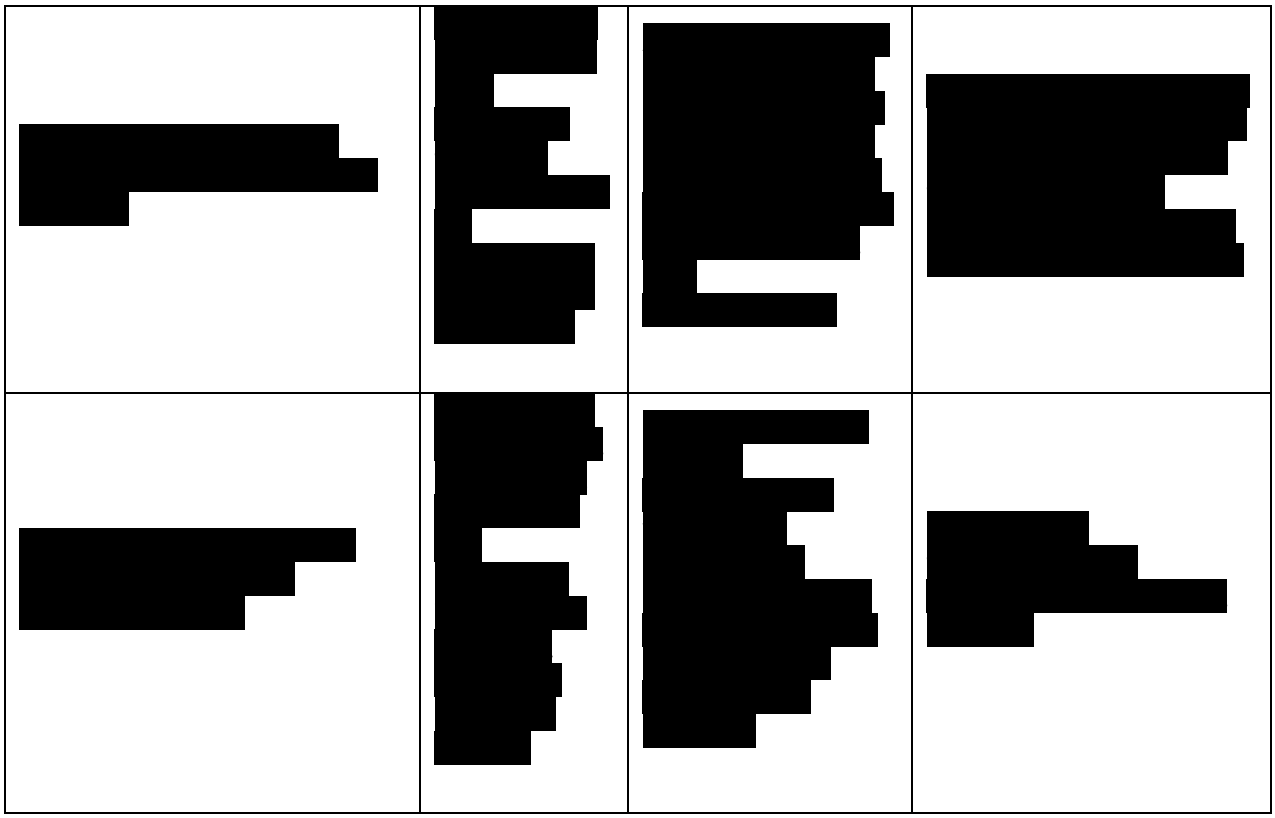
ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASI01	
(Nombre del sistema A1)	Sistema de inventarios FCA	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASI01		
(Nombre del sistema A1)	Sistema de inventarios FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**

[2] **Texto eliminado:** Apartado correspondiente a "Análisis de Brecha y del Plan de Trabajo" (páginas 5 a 6). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.



MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASI01
(Nombre del sistema A1)	Sistema de inventarios FCA
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	El sistema no requiere la realización de transferencias de datos personales mediante el traslado de soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	El sistema no requiere la realización de transferencias de datos personales mediante el traslado de soportes electrónicos

[3] **Texto eliminado:** Apartado correspondiente a "Análisis de Brecha y del Plan de Trabajo" (páginas 5 a 6). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Transferencias mediante el traslado sobre redes electrónicas:	El sistema no requiere la realización de transferencias de datos personales sobre redes electrónicas

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**

   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;

   No se registran bitácoras en el sistema.
   b) Para soportes físicos: Número o clave del expediente utilizado, y
   No aplica
   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
   No aplica

2. Si las bitácoras están en soporte físico o en soporte electrónico;
   No se registran bitácoras en el sistema
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
   En el sistema operativo de red de manera semanal
4. La manera en que asegura la integridad de las bitácoras, y
   Con respaldos semanales
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
   Administrador de servidores
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
   No hay herramientas de análisis

III. ACCESO A LAS INSTALACIONES

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado.

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales

IV. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
Sí
b) ¿Es discrecional (matriz de control de acceso)?
Sí
c) ¿Está basado en roles (perfiles) o grupos?
Sí
d) ¿Está basado en reglas?
Sí

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo contraseñas

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo contraseñas

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema
b) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema
c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí
c) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

V. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos X , diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual _X__,
   c) Periodicidad con que los realiza: semanal
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Discos duros
3. Cómo y dónde archiva esos medios
   Arreglos de discos
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Administrador de servidores

VI. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   No se cuenta con plan de contingencia, pero se planea desarrollarlo.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   No aplica

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASI01	
(Nombre del sistema A1)	Sistema de inventarios FCA	
Recurso	**Descripción**	**Control**
NANGIOS	*Monitorea los recursos y servicios de los servidores*	*Lo lleva a cabo el administrador de servidores* Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASI01	
(Nombre del sistema A1)	Sistema de inventarios FCA	
Medida de seguridad	**Procedimiento***	**Responsable***
No aplica	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único*	FCASI01	
(Nombre del sistema A1)	Sistema de inventarios FCA	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASI01	
(Nombre del sistema A1)	Sistema de inventarios FCA	
Medida de seguridad	**Acciones***	**Responsable***
No aplica	*No aplica*	*a) No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASI01		
(Nombre del sistema A1)	Sistema de inventarios FCA		
Actividad*	**Descripción***	**Duración***	**Cobertura***
La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASI01		
(Nombre del sistema A1)	Sistema de inventarios FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir enlace a el aviso de privacidad	*Se realiza de manera electrónica*	*Permanente*	*Usuarios del sistema*

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASI01

(Nombre del sistema A1)	Sistema de inventarios FCA		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso de privacidad vigente*	*Permanente*	*Usuarios del sistema*

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASI01		
(Nombre del sistema A1)	Sistema de inventarios FCA		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Instalación de parches de seguridad	*Se descargan e instalan de manera manual*	*Cada que se recibe notificación de un nuevo parche de seguridad*	*Mantener la integridad de los datos ante amenazas*
Limpieza de logs	*Se elimina información histórica de bitácoras*	*Mensual*	*Ayuda a liberar espacio de almacenamiento*

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASI01	
(Nombre del sistema A1)	Sistema de inventarios FCA	
Proceso	**Descripción**	**Responsable**

Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes* *Copiar un nuevo respaldo*	*a) Administrador de servidores*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASI01	
(Nombre del sistema A1)	Sistema de inventarios FCA	
Proceso	**Descripción**	**Responsable**
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	*a)* Administrador de servidores

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A2 SISTEMA DE REPORTES DE SOPORTE TÉCNICO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASISOP01
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre de los responsables para uso de un bien de la Facultad (académicos de tiempo completo y personal administrativo)
Responsable*:	
Nombre*:	**Balfred Santaella Hinojosa**
Cargo*:	**Jefe del Centro de Informática**
Funciones*:	Planeación, organización y control de los sistemas de información de la Facultad.
Obligaciones*:	Asegurar el funcionamiento de los sistemas y servicios de información.
	Encargados:
(Nombre del Encargado 1)	**Víctor Hugo Carrillo López**
Cargo:	**Responsable de Soporte Técnico**
Funciones:	Soporte en la base de datos de nombre y apellidos de los académicos de tiempo completo y personal administrativo adscrito a la FCA para poder establecer un vínculo con el equipo de cómputo o periférico para registrar reportes y seguimiento de servicios.
Obligaciones:	Validar y mantener la confidencialidad de los datos personales (nombre y apellidos) para uso exclusivo del registro de los servicios realizados por el departamento. Asegurar la integridad de la información de datos personales registrada en la base de datos del sistema.
	Usuarios:
(Nombre del Usuario 1)	**Víctor Hugo Carrillo López**
Cargo:	Responsable de Soporte Técnico
Funciones:	Utilizar únicamente el nombre de un académico de tiempo completo o personal administrativo para registrarle un reporte de atención por parte del departamento de soporte técnico.
Obligaciones:	Mantener la confidencialidad de los datos personales (nombre y apellidos) para uso exclusivo del registro de los servicios realizados por el departamento.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASISOP01
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico
Tipo de soporte:	Soporte electrónico.
Descripción:	Soporte electrónico: base de datos relacional.
Características del lugar donde se resguardan los soportes:*	Soporte electrónico: base de datos relacional en un servidor ubicado en el Centro de Informática de la FCA.

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASISOP01	
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico	
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]

ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASISOP01	
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]

[5] **Texto eliminado:** Apartado correspondiente a "Análisis de Riesgos y Análisis de Brecha" (páginas 15 a 16). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

[redacted]		
[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASISOP01		
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico		
Actividad	**Descripción**	**Duración**	**Cobertura**
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[6] **Texto eliminado:** Apartado correspondiente a "Análisis de Brecha y del Plan de Trabajo" (páginas 16 a 17). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

	[redacted]	[redacted]	

MEDIDAS DE SEGURIDAD IMPLEMENTADAS

TRANSFERENCIAS DE DATOS PERSONALES

Sistema de Reportes de Soporte Técnico

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASISOP01
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	El sistema no requiere la realización de transferencias de datos personales mediante el traslado de soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	El sistema no requiere la realización de transferencias de datos personales mediante el traslado de soportes electrónicos
Transferencias mediante el traslado sobre redes electrónicas:	El sistema no requiere la realización de transferencias de datos personales sobre redes electrónicas

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado

Seguridad perimetral
Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales

PERFILES DE USUARIO Y CONTRASEÑAS

[7] **Texto eliminado:** Apartado correspondiente a "Análisis de Brecha y del Plan de Trabajo" (páginas 16 a 17). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

1. Modelo de control de acceso (alguno de los siguientes):

e) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
Sí
f) ¿Es discrecional (matriz de control de acceso)?
Sí
g) ¿Está basado en roles (perfiles) o grupos?
Sí
h) ¿Está basado en reglas?
Sí

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

d) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
e) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
f) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo contraseñas

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

c) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí
d) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo contraseñas

4. Administración de perfiles de usuario y contraseñas:

d) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema
e) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema
f) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:

d) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
e) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí
f) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

5. Señalar si realiza respaldos

d) Completos X , diferenciales ___ o incrementales___;
e) De forma automática ____ o Manual _X__,
f) Periodicidad con que los realiza: _semanal_

6. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;[8]
   Discos duros
7. Cómo y dónde archiva esos medios,
   Arreglos de discos
8. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Administrador de servidores

PLAN DE CONTINGENCIA

No se cuenta con plan de contingencia, pero se planea desarrollarlo

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASISOP01	
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico	
Recurso	**Descripción**	**Control**
NANGIOS	*Monitorea los recursos y servicios de los servidores*	*Lo lleva a cabo el administrador de servidores* Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASISOP01
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico

Es deseable que precise si para almacenar dichos medios cuenta con al menos dos lugares distintos que cumplan con las condiciones de seguridad especificadas en el articulado del Capítulo V de los Lineamientos, conforme a la fracción III del Trigésimo primero de los Lineamientos; o bien, si utiliza un espacio externo seguro para guardar de manera sistemática dichos respaldos, según la fracción VIII del Trigésimo séptimo de tales Lineamientos.

Medida de seguridad	Procedimiento	Responsable
No aplica	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASISOP01	
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASISOP01	
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*b) No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASISOP01

(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico		
Actividad	**Descripción**	**Duración**	**Cobertura**
La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASISOP01		
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir enlace a el aviso de privacidad	*Se realiza de manera electrónica*	*Permanente*	*Usuarios del sistema*

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASISOP01		
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven	*Actualizar el acceso de manera electrónica a la*	*Permanente*	*Usuarios del sistema*

a cabo en el aviso de privacidad	*versión más reciente del aviso de privacidad vigente*		

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASISOP01		
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	*Se descargan e instalan de manera manual*	*Cada que se recibe notificación de un nuevo parche de seguridad*	*Mantener la integridad de los datos ante amenazas*
Limpieza de logs	*Se elimina información histórica de bitácoras*	*Mensual*	*Ayuda a liberar espacio de almacenamiento*

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASISOP01	
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico	
Proceso*	**Descripción***	**Responsable***
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes*	*b) Administrador de servidores*

	Copiar un nuevo respaldo	

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASISOP01	
(Nombre del sistema A2)	Sistema de Reportes de Soporte Técnico	
Proceso	**Descripción**	**Responsable**
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	*b)* Administrador de servidores

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A3 SISTEMA DE LA PLATAFORMA PARA PROCESOS DE ACREDITACIÓN DE LA FCA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCAPA01
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA
Datos personales (sensibles o no) contenidos en el sistema*:	Nombres, firmas y número de trabajador del personal académico de asignatura y de tiempo completo. Nombre de alumnos.
Responsable:	
Nombre:	**Balfred Santaella Hinojosa**
Cargo:	**Jefe del Centro de Informática**
Funciones:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1)	Raúl Esteban Cruz Quiroz

Cargo:	Responsable de Infraestructura
Funciones:	Soporte de documentos electrónicos que contienen datos personales de personal académico adscrito a la FCA, estudiantes y egresados.
Obligaciones:	Validar y mantener la confidencialidad de los datos personales para uso exclusivo de procesos de acreditación de la institución.
	Usuarios:
(Nombre del Usuario 1)	Beatriz Sánchez Osornio
Cargo:	Jefa del Departamento de Acreditaciones
Funciones*:	Acceso a expedientes con nombres, firmas, grados académicos y número de trabajador de los académicos de la FCA. Acceso a listados con nombres, firmas y número de cuenta de alumnos de la FCA.
Obligaciones:	Mantener la confidencialidad de los datos personales para uso exclusivo de procesos de acreditación de la institución.
(Nombre del Usuario 2)	Bibiana Marlen Bahena González Diana Vianey Durán Hernández Gustavo Ángel Jiménez de la Cerda Mauricio Piña Prudencio Juan Carlos Secundino Estrada Julián Edgar Valente Antonio
Cargo:	Coordinador de Información
Funciones:	Testar los documentos que contienen nombres, firmas y número de trabajador de los académicos de la FCA. Testar los documentos que contienen nombres, firmas y número de cuenta de alumnos de la FCA.
Obligaciones:	Mantener la confidencialidad de los datos personales para uso exclusivo de procesos de acreditación de la institución.
(Nombre del Usuario 3)	Acreditador
Cargo:	Acreditador
Funciones:	Revisión de expedientes testados de nombres, firmas, grados académicos y número de trabajador de los académicos de la FCA, únicamente para verificar su utilidad como evidencia documental en respuesta al instrumento de evaluación para la acreditación. Revisión de listados testados de nombres, firmas y número de cuenta de alumnos de la FCA, para verificar que sirven de evidencia documental de la respuesta que la institución proporciona para validar el instrumento de acreditación.
Obligaciones:	Mantener la confidencialidad de los datos personales para uso exclusivo de procesos de acreditación de la institución de acuerdo con las cláusulas de privacidad y confidencialidad del contrato celebrado entre la agencia de acreditación y la institución.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCAPA01
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA
Tipo de soporte:	Soporte electrónico.
Descripción:	Soporte electrónico: base de datos relacional y archivos testados en Portable Document Format (PDF)
Características del lugar donde se resguardan los soportes:	Soporte electrónico: base de datos relacional en un servidor ubicado en el Centro de Informática de la FCA y árbol de directorios en un servidor ubicado en el Centro de Informática.

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCAPA01	
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA	
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]

ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCAPA01	
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]

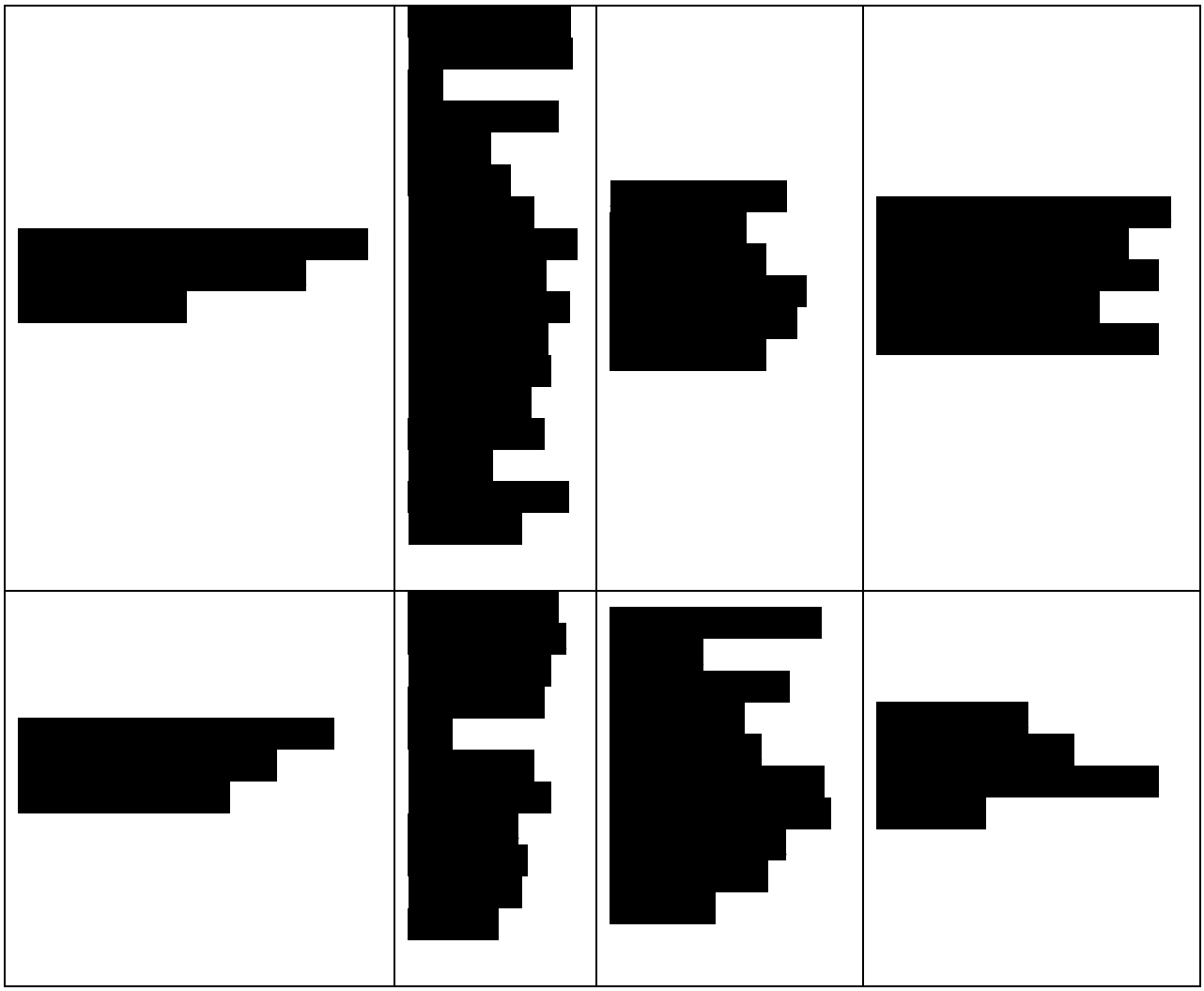
[9] **Texto eliminado:** Apartado correspondiente a “Análisis de Riesgos y de Análisis de Brecha” (páginas 26 a 27). **Fundamento legal y motivación:** artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCAPA01		
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**
[redacted]	[redacted]	[redacted]	[redacted]

[10] **Texto eliminado:** Apartado correspondiente a "Análisis de Brecha y del Plan de Trabajo" (páginas 27 a 28). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.



MEDIDAS DE SEGURIDAD IMPLEMENTADAS

TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCAPA01
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	El sistema no requiere la realización de transferencias de datos personales mediante el traslado de soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	El sistema no requiere la realización de transferencias de datos personales mediante el traslado de soportes electrónicos

[12] **Texto eliminado:** Apartado correspondiente a “Análisis de Brecha y del Plan de Trabajo” (páginas 27 a 28). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Transferencias mediante el traslado sobre redes electrónicas:	El sistema no requiere la realización de transferencias de datos personales sobre redes electrónicas

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado

Seguridad perimetral interior

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales

PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

i) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
Sí
j) ¿Es discrecional (matriz de control de acceso)?
Sí
k) ¿Está basado en roles (perfiles) o grupos?
Sí
l) ¿Está basado en reglas?
Sí

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

g) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
h) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
i) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo contraseñas

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

e) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí
f) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

Sólo contraseñas

4. Administración de perfiles de usuario y contraseñas:

g) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema

h) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema

i) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:

g) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

h) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí

i) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

9. Señalar si realiza respaldos

g) Completos_X , diferenciales ___ o incrementales___;

h) De forma automática ____ o Manual _X__,

i) Periodicidad con que los realiza: _semanal_

10. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad·
Discos duros

11. Cómo y dónde archiva esos medios, y
Arreglos de discos

12. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
Administrador de servidores

PLAN DE CONTINGENCIA

No se cuenta con plan de contingencia, pero se planea desarrollarlo

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCAPA01

(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA	
Recurso	**Descripción**	**Control**
NANGIOS	*Monitorea los recursos y servicios de los servidores*	*Lo lleva a cabo el administrador de servidores* Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCAPA01	
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA	
Medida de seguridad	**Procedimiento**	**Responsable**
No aplica	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCAPA01	
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCAPA01	
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCAPA01		
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**
La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCAPA01
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA

Actividad	Descripción	Duración	Cobertura
Incluir enlace a el aviso de privacidad	*Se realiza de manera electrónica*	*Permanente*	*Usuarios del sistema*

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCAPA01		
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso de privacidad vigente*	*Permanente*	*Usuarios del sistema*

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCAPA01		
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	*Se descargan e instalan de manera manual*	*Cada que se recibe notificación de un nuevo parche de seguridad*	*Mantener la integridad de los datos ante amenazas*

Limpieza de logs	*Se elimina información histórica de bitácoras*	*Mensual*	*Ayuda a liberar espacio de almacenamiento*

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCAPA01	
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA	
Proceso	**Descripción**	**Responsable**
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes* *Copiar un nuevo respaldo*	*c) Administrador de servidores*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCAPA01	
(Nombre del sistema A3)	Plataforma para procesos de acreditación de la FCA	
Proceso	**Descripción**	**Responsable**
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	*c)* Administrador de servidores

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A4 SISTEMA DE ADMINISTRACIÓN DE LA LIBRERÍA DE LA FCA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASAL01
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA
Datos personales (sensibles o no) contenidos en el sistema:	Nombres y apellidos de los usuarios del sistema. No se registran datos personales de académicos, alumnos o público en general.
Responsable:	
Nombre:	**Balfred Santaella Hinojosa**
Cargo:	**Jefe del Centro de Informática**
Funciones:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1)	**Raúl Esteban Cruz Quiroz**
Cargo:	**Responsable de Infraestructura**
Funciones:	Soporte en la base de datos de nombre y apellidos de los usuarios del sistema.
Obligaciones:	Asegurar la integridad y confidencialidad de la información de datos personales (nombres y apellidos) de los usuarios del sistema.
	Usuarios:
(Nombre del Usuario 1)	Coordinadora de Promoción Editorial Jennifer Elein Esquivel Valdepeña y López Asistente en Librería Nancy Villarruel Palma
Cargo:	Coordinadora de Promoción Editorial, Asistente en Librería
Funciones*:	No hay funciones con relación al trato de datos personales, solo realiza la gestión del inventario (entradas y salidas de libros)
Obligaciones:	No hay obligaciones con relación al trato de datos personales
(Nombre del Usuario 2)	Asistente en Librería Nancy Villarruel Palma

	Punto de venta Héctor Aniceto López Rubén Colin Martínez Rosa María León Meza Sergio Monroy Palma Daniel Ortiz Garibay Arístides Rodríguez Martínez Rocío Valdez González Aried Vidal Rodríguez
Cargo:	Asistente en Librería, Punto de venta
Funciones:	No hay funciones con relación al trato de datos personales
Obligaciones:	No hay obligaciones con relación al trato de datos personales

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASAL01
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA
Tipo de soporte:	Soporte electrónico.
Descripción:	Soporte electrónico: base de datos relacional
Características del lugar donde se resguardan los soportes:	Soporte electrónico: base de datos relacional en un servidor ubicado en el Centro de Informática de la FCA

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASAL01	
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA[13]	
Riesgo	**Impacto**	**Mitigación**

[13] **Texto eliminado:** Apartado correspondiente a "Análisis de Riesgos" (página 36). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

[redacted]	[redacted]	[redacted]

ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASAL01	
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)

[14] **Texto eliminado:** Apartado correspondiente a "Análisis de Riesgos, de Análisis de Brecha y del Plan de Trabajo" (páginas 37 a 38). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Identificador único	FCASAL01		
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

MEDIDAS DE SEGURIDAD IMPLEMENTADAS

TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASAL01
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	El sistema no requiere la realización de transferencias de datos personales mediante el traslado de soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	El sistema no requiere la realización de transferencias de datos personales mediante el traslado de soportes electrónicos

[15] **Texto eliminado:** Apartado correspondiente a “Plan de Trabajo” (página 38). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Transferencias mediante el traslado sobre redes electrónicas:	El sistema no requiere la realización de transferencias de datos personales sobre redes electrónicas

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales

PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

m) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
Sí
n) ¿Es discrecional (matriz de control de acceso)?
Sí
o) ¿Está basado en roles (perfiles) o grupos?
Sí
p) ¿Está basado en reglas?
Sí

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

j) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
k) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
l) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo contraseñas

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

g) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí
h) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo contraseñas

4. Administración de perfiles de usuario y contraseñas:

j) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema
k) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema
l) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:
j) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
k) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí
l) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

13. Señalar si realiza respaldos
j) Completos_X , diferenciales ___ o incrementales___;
k) De forma automática ____ o Manual _X__,
l) Periodicidad con que los realiza: _semanal_
14. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
Discos duros
15. Cómo y dónde archiva esos medios, y
Arreglos de discos
16. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
Administrador de servidores

PLAN DE CONTINGENCIA

No se cuenta con plan de contingencia, pero se planea desarrollarlo

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASAL01	
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA	
Recurso	**Descripción**	**Control**

NANGIOS	*Monitorea los recursos y servicios de los servidores*	*Lo lleva a cabo el administrador de servidores* Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASAL01	
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA	
Medida de seguridad	**Procedimiento**	**Responsable**
No aplica	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASAL01	
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASAL01

(Nombre del sistema A4)	Sistema de administración de la librería de la FCA	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*c) No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASAL01		
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**
La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

(Denominación del área específica del Área Universitaria A)*			
Identificador único	FCASAL01		
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir enlace a el aviso de privacidad	*Se realiza de manera electrónica*	*Permanente*	*Usuarios del sistema*

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASAL01		
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso de privacidad vigente*	*Permanente*	*Usuarios del sistema*

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASAL01		
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	*Se descargan e instalan de manera manual*	*Cada que se recibe notificación de un nuevo parche de seguridad*	*Mantener la integridad de los datos ante amenazas*
Limpieza de logs	*Se elimina información histórica de bitácoras*	*Mensual*	*Ayuda a liberar espacio de almacenamiento*

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASAL01	
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA	
Proceso	**Descripción**	**Responsable**
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes* *Copiar un nuevo respaldo*	*d) Administrador de servidores*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASAL01	
(Nombre del sistema A4)	Sistema de administración de la librería de la FCA	
Proceso	**Descripción**	**Responsable**
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	*d)* Administrador de servidores

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A5 SISTEMA DE ADMINISTRACIÓN DOCENTE

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASAD01
(Nombre del sistema A5)	Sistema de Administración Docente

Datos personales (sensibles o no) contenidos en el sistema:	Nombre, número de trabajador, fotografía del rostro y biométricos (huella digital) del personal académico de asignatura y de tiempo completo
Responsable:	
Nombre:	**Balfred Santaella Hinojosa**
Cargo:	**Jefe del Centro de Informática**
Funciones*:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones*:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1)	Raúl Esteban Cruz Quiroz
Cargo:	Responsable de Infraestructura
Funciones:	Soporte en la base de datos de nombre y apellidos, números de trabajador y biométricos de huella digital de los académicos de la FCA para acreditar el registro de asistencia a clases y jornada de tiempo completo, así como también para la emisión de reportes de asistencias.
Obligaciones:	Validar y mantener la confidencialidad de los datos personales (nombre y apellidos, números de trabajador y biométricos de huella digital) para la emisión de reportes de asistencias del personal académico.
	Usuarios:
(Nombre del Usuario 1)	Jefa de Control Docente y Programas Institucionales Beatriz Adriana Flores Muñoz Coordinador de Control Docente y Programas Institucionales Alejandro Téllez Sánchez Coordinador del SUAyED Sara Guadalupe Espinosa de los Monteros Montes de Oca Apoyo a la Coordinación Modalidad Abierta del SUAyED Óscar René González Urrutia Coordinadora de Admisión e Informes de la División de Estudios de Posgrado María Eugenia Patiño Navarro
Cargo:	Jefa de Control Docente y Programas Institucionales, Coordinador de Control Docente y Programas Institucionales, Coordinador del SUAyED, Apoyo a la Coordinación Modalidad Abierta del SUAyED, Coordinadora de Admisión e Informes de la División de

	Estudios de Posgrado
Funciones:	Asociar los nombres y números de trabajador de los académicos con un registro biométrico de huella digital para que los docentes puedan registrar asistencia.
Obligaciones:	Mantener confidencialidad de los datos personales de los académicos y sus registros históricos de asistencia.
(Nombre del Usuario 2)	Jefa de Control Docente y Programas Institucionales Beatriz Adriana Flores Muñoz Coordinador de Control Docente y Programas Institucionales Alejandro Téllez Sánchez Asistente de la Sala de Profesores Emma Alcantar Mora Juan Carlos Contreras Segundo Sofía Peña Herrera Coordinador del SUAyED Sara Guadalupe Espinosa de los Monteros Montes de Oca Apoyo a la Coordinación Modalidad Abierta del SUAyED Óscar René González Urrutia Apoyo Sala de Firmas de la División de Estudios de Posgrado Mónica Ivonne García Rodríguez
Cargo:	Jefa de Control Docente y Programas Institucionales, Coordinador de Control Docente y Programas Institucionales, Asistente de la Sala de Profesores, Coordinador del SUAyED, Apoyo a la Coordinación Modalidad Abierta del SUAyED, Apoyo Sala de Firmas de la División de Estudios de Posgrado
Funciones:	Asegurar el funcionamiento de los equipos de registro de diario de asistencia y monitores de informe de asistencia al horario activo de clase, exclusivamente en las salas de firmas designadas para esa labor.
Obligaciones:	Mantener confidencialidad de los datos personales de los académicos de asignatura que se proyectan en los monitores de informe de asistencia al horario activo de clase.
(Nombre del Usuario 3)	Jefa de Control Docente y Programas Institucionales Beatriz Adriana Flores Muñoz Coordinador de Control Docente y Programas Institucionales Alejandro Téllez Sánchez
Cargo:	Jefa de Control Docente y Programas Institucionales, Coordinador de Control Docente y Programas Institucionales.
Funciones:	Imprimir reportes de asistencias para la tramitación de estímulos de los académicos de tiempo completo y de asignatura.

Obligaciones:	Mantener confidencialidad de los datos personales de los académicos de asignatura y sus registros históricos de asistencia.
(Nombre del Usuario 4)	Jefa de Control Docente y Programas Institucionales Beatriz Adriana Flores Muñoz Coordinador de Control Docente y Programas Institucionales Alejandro Téllez Sánchez Apoyo a la Coordinación Modalidad Abierta del SUAyED Óscar René González Urrutia Apoyo a la Coordinación Modalidad a Abierta del SUAyED Alejandra Altamirano Román Apoyo a la Coordinación Modalidad a Distancia del SUAyED Erika Angelina Nuevo Esteves Apoyo Sala de Firmas de la División de Estudios de Posgrado Mónica Ivonne García Rodríguez
Cargo:	Jefa de Control Docente y Programas Institucionales, Coordinador de Control Docente y Programas Institucionales, Apoyo a la Coordinación Modalidad Abierta del SUAyED, Apoyo a la Coordinación Modalidad a Abierta del SUAyED, Apoyo a la Coordinación Modalidad a Distancia del SUAyED, Apoyo Sala de Firmas de la División de Estudios de Posgrado
Funciones:	Registro de incidencias para la justificación de inasistencias de los académicos y programación de reposiciones para compensar sesiones no impartidas por los docentes.
Obligaciones:	Mantener confidencialidad de los datos personales de los académicos y los registros históricos de asistencia.
(Nombre del Usuario 5)	Jefe de División Alfonso Ayala Rico Rosa Martha Barona Peña Silvia Berenice Villamil Rodríguez María del Rocío Huitrón Hernández Coordinador de licenciatura Alfonso Manuel Aguilar Guevara María Gloria Arévalo Guerrero Eva Elizabeth del Valle Córdova Graciela Enríquez Guadarrama Gabriel Guevara Gutiérrez Javier Isaac Osorio González Francisco Alberto Piña Salazar Pedro Eduardo Quezada García María Angélica Alicia Raya Sánchez Isaías Reyes Bojórquez Carlos Ruiz Díaz Carlos Ríos Murillo Alma Lucero Sosa Blancas

	Karen Gisel Velázquez Rojas Israel Vladimir Villa García Romeo Vite López
Cargo:	Jefe de División y Coordinador académico de licenciatura
Funciones:	Monitoreo en tiempo real de los registros de asistencia de los académicos de la FCA.
Obligaciones:	Mantener confidencialidad de los datos personales de los académicos de asignatura y sus registros históricos de asistencia.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASAD01
(Nombre del sistema A5)	Sistema de Administración Docente
Tipo de soporte:	Soporte físico y electrónico.
Descripción:	Soporte físico: Reportes de asistencias Soporte electrónico: base de datos relacional
Características del lugar donde se resguardan los soportes:	Soporte electrónico: base de datos relacional en un servidor ubicado en el Centro de Informática de la FCA

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASAD01	
(Nombre del sistema A5)	Sistema de Administración Docente[16]	
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]

[16] **Texto eliminado:** Apartado correspondiente a "Análisis de Riesgos" (página 48). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

		[redacted]

ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASAD01	
(Nombre del sistema A5)	Sistema de Administración Docente[17]	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

[17] **Texto eliminado:** Apartado correspondiente a "Análisis de Riesgos, de Análisis de Brecha y del Plan de Trabajo" (páginas 49 a 50). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASAD01		
(Nombre del sistema A5)	Sistema de Administración Docente		
Actividad	**Descripción**	**Duración**	**Cobertura**
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

MEDIDAS DE SEGURIDAD IMPLEMENTADAS

TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASAD01
(Nombre del sistema A5)	Sistema de Administración Docente
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	El sistema no requiere la realización de transferencias de datos personales mediante el traslado de soportes físicos

[18] **Texto eliminado:** Apartado correspondiente a “Plan de Trabajo” (página 50). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Transferencias mediante el traslado de soportes electrónicos:	El sistema no requiere la realización de transferencias de datos personales mediante el traslado de soportes electrónicos
Transferencias mediante el traslado sobre redes electrónicas:	El sistema no requiere la realización de transferencias de datos personales sobre redes electrónicas

RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales

PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

q) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
Sí
r) ¿Es discrecional (matriz de control de acceso)?
Sí
s) ¿Está basado en roles (perfiles) o grupos?
Sí
t) ¿Está basado en reglas?
Sí

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

m) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
n) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
o) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo contraseñas

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

i) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí

j) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo contraseñas

4. Administración de perfiles de usuario y contraseñas:
m) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema
n) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema
o) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:
m) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
n) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí
o) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

17. Señalar si realiza respaldos
m) Completos_X , diferenciales ___ o incrementales___;
n) De forma automática ____ o Manual _X__,
o) Periodicidad con que los realiza: _semanal_
18. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;
Discos duros
19. Cómo y dónde archiva esos medios, y
Arreglos de discos
20. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
Administrador de servidores

PLAN DE CONTINGENCIA

3. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
No se cuenta con plan de contingencia, pero se planea desarrollarlo
4. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
No aplica
5. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
a) El tipo de sitio (caliente, tibio o frío);
b) Si el sitio es propio o subcontratado con un tercero;
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

No aplica

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

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASAD01	
(Nombre del sistema A5)	Sistema de Administración Docente	
Recurso	**Descripción**	**Control**
NANGIOS	*Monitorea los recursos y servicios de los servidores*	*Lo lleva a cabo el administrador de servidores* Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASAD01	
(Nombre del sistema A5)	Sistema de Administración Docente	
Medida de seguridad	**Procedimiento**	**Responsable**
No aplica	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASAD01
(Nombre del sistema A5)	Sistema de Administración Docente

Medida de seguridad	Resultado de evaluación	Responsable
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASAD01	
(Nombre del sistema A5)	Sistema de Administración Docente	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*d) No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASAD01		
(Nombre del sistema A5)	Sistema de Administración Docente		
Actividad	**Descripción**	**Duración**	**Cobertura**
La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASAD01		
(Nombre del sistema A5)	Sistema de Administración Docente		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir enlace a el aviso de privacidad	*Se realiza de manera electrónica*	*Permanente*	*Usuarios del sistema*

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASAD01		
(Nombre del sistema A5)	Sistema de Administración Docente		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso de privacidad vigente*	*Permanente*	*Usuarios del sistema*

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASAD01

(Nombre del sistema A5)	Sistema de Administración Docente		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	*Se descargan e instalan de manera manual*	*Cada que se recibe notificación de un nuevo parche de seguridad*	*Mantener la integridad de los datos ante amenazas*
Limpieza de logs	*Se elimina información histórica de bitácoras*	*Mensual*	*Ayuda a liberar espacio de almacenamiento*

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASAD01	
(Nombre del sistema A5)	Sistema de Administración Docente	
Proceso	**Descripción**	**Responsable**
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes* *Copiar un nuevo respaldo*	*e) Administrador de servidores*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASAD01
(Nombre del sistema A5)	Sistema de Administración Docente

Proceso	Descripción	Responsable
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	*e)* Administrador de servidores

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A6 SISTEMA DEL PROGRAMA PERMANENTE DE CAPACITACIÓN A DISTANCIA PARA PROFESORES DE LA FCA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASPPCDP01**
(Nombre del sistema A6)	Sistema del Programa Permanente de Capacitación a Distancia para Profesores de la FCA
Datos personales (sensibles o no) contenidos en el sistema:	Datos del trabajador y datos de los cursos de capacitación que ha tomado Nombre, apellido paterno, apellido materno, numero de trabajador, RFC y CURP
Responsable:	
Nombre:	**Balfred Santaella Hinojosa**
Cargo:	**Jefe del Centro de Informática**
Funciones:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1)	**Adriana García Vargas**
Cargo:	**Coordinadora de Laboratorios**
Funciones:	Soporte al área para la automatización de datos personales de los académicos que desean tomar cursos. Manejo de la base de datos.
Obligaciones*:	Almacenamiento e integridad de la información. Emplear los datos personales dentro del proceso definido y para los fines del sistema.
	Usuarios:

(Nombre del Usuario 1*)	**Académicos de la FCA**
Cargo:	Son todos aquellos que cuentan con un nombramiento académico
Funciones:	
Obligaciones:	
(Nombre del Usuario 2)	Rocío Ayme García Castillo
Cargo:	Coordinadora de Cursos de Capacitación Especializados
Funciones:	**Administrador del sistema**
Obligaciones:	Emplear los datos personales dentro del proceso definido y para los fines del sistema.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (FCA)	
Identificador único	**FCASPPCDP01**
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA
Tipo de soporte:	Electrónico
Descripción:	Sistema de información
Características del lugar donde se resguardan los soportes:	Sitio dentro del Centro de Informática de la FCA ubicado en la planta baja, cuenta con aire acondicionado a 18° centígrados, el acceso es con puerta de marco laminado y con vidrio, cuenta con una cerradura sencilla, la llave y la copia es manejada por el Administrador de Servidores y el jefe del Centro de Informática.

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (FCA)		
Identificador único	**FCASPPCDP01**	
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA[19]	
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]

[19] **Texto eliminado:** Apartado correspondiente a "Análisis de Riesgos" (página 58). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

		[redacted]
[redacted]	[redacted]	[redacted]

ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (FCA)		
Identificador único	**FCASPPCDP01**	
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (FCA)			
Identificador único	**FCASPPCDP01**		
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**

[20] **Texto eliminado:** Apartado correspondiente a “Análisis de Riesgos, de Análisis de Brecha y del Plan de Trabajo” (páginas 59 a 60). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

[redacted]	[redacted]	[redacted]	[redacted]

MEDIDAS DE SEGURIDAD IMPLEMENTADAS

TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (FCA)	
Identificador único	**FCASPPCDP01**
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica, no se reciben documentos o expedientes físicos.

RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Nombre	Cargo	Funciones	Obligaciones
Mtro. Balfred Santaella Hinojosa	Jefe del Centro de Informática	Planeación, organización y control de los sistemas de información de la Facultad.	Asegurar el funcionamiento de los sistemas y servicios de información.
Mtro. Germán Ignacio Cervantes González	Administrador de Servidores	Gestión, configuración, mantenimiento y soporte de los servidores y las bases de datos.	Revisar y mantener la correcta operación y disponibilidad de los servicios que dan soporte a los distintos sistemas de información.

[21] **Texto eliminado:** Apartado correspondiente a “Plan de Trabajo” (página 60). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales

PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

u) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
Sí
v) ¿Es discrecional (matriz de control de acceso)?
Sí
w) ¿Está basado en roles (perfiles) o grupos?
Sí
x) ¿Está basado en reglas?
Sí

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

p) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
q) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
r) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo contraseñas

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

k) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Sí
l) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sólo contraseñas

4. Administración de perfiles de usuario y contraseñas:

p) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema
q) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema
r) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:

p) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
q) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí
r) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

21. Señalar si realiza respaldos
- **p)** Completos_X , diferenciales ___ o incrementales___;
- **q)** De forma automática ____ o Manual _X__,
- **r)** Periodicidad con que los realiza: _semanal_

22. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
Discos duros

23. Cómo y dónde archiva esos medios, y
Arreglos de discos

24. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
Administrador de servidores

PLAN DE CONTINGENCIA

No se cuenta con plan de contingencia, pero se planea desarrollarlo

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

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (FCA)		
Identificador único	**FCASPPCDP01**	
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA	
Recurso	**Descripción**	**Control**
NANGIOS	*Monitorea los recursos y servicios de los servidores*	*Lo lleva a cabo el administrador de servidores* Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (FCA)		
Identificador único	**FCASPPCDP01**	
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA	
Medida de seguridad	**Procedimiento**	**Responsable**
No aplica	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (FCA)		
Identificador único	**FCASPPCDP01**	
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (FCA)	
Identificador único	**FCASPPCDP01**
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA

Medida de seguridad	Acciones	Responsable
No aplica	*No aplica*	*No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (FCA)			
Identificador único	**FCASPPCDP01**		
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**
La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (FCA)			
Identificador único	**FCASPPCDP01**		
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir enlace a el aviso de privacidad	*Se realiza de manera electrónica*	*Permanente*	*Usuarios del sistema*

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (FCA)			
Identificador único	**FCASPPCDP01**		
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso de privacidad vigente*	*Permanente*	*Usuarios del sistema*

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (FCA)			
Identificador único	**FCASPPCDP01**		
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	*Se descargan e instalan de manera manual*	*Cada que se recibe notificación de un nuevo parche de seguridad*	*Mantener la integridad de los datos ante amenazas*
Limpieza de logs	*Se elimina información histórica de bitácoras*	*Mensual*	*Ayuda a liberar espacio de almacenamiento*

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (FCA)		
Identificador único	**FCASPPCDP01**	
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA	
Proceso	**Descripción**	**Responsable**
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes* *Copiar un nuevo respaldo*	*Administrador de servidores*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (FCA)		
Identificador único	**FCASPPCDP01**	
(Nombre del sistema A6)	Programa Permanente de Capacitación a Distancia para Profesores de la FCA	
Proceso	**Descripción**	**Responsable**
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	Administrador de servidores

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A7 SISTEMA DE BOLSA DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (FCA)	
Identificador único	FCASIBT01
(Nombre del sistema A7)	Sistema de Bolsa de Trabajo
Datos personales (sensibles o no) contenidos en el sistema:	Datos de identificación. • De aspirantes: Nombre, domicilio, correo, teléfono, estado civil, fecha de nacimiento. • De empresas: Razón social, Domicilio, Teléfono, Nombre del reclutador, puesto, correo y horario de atención. Datos laborales. De aspirantes: Experiencia laboral, idiomas, cursos especializados.
Responsable:	
Nombre:	**Mtro. Balfred Santaella Hinojosa**
Cargo:	**Jefe del Centro de Informática**
Funciones:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones*:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1)	**Mtro. Hugo Díaz García**
Cargo:	Jefe de Sistemas
Funciones:	Soporte al área para la automatización de datos personales de los candidatos (alumnos), reclutadores y las empresas. Manejo de la base de datos.
Obligaciones:	Almacenamiento e integridad de la información. Emplear los datos personales dentro del proceso definido y para los fines del sistema.
	Usuarios
(Nombre del Usuario 1)	Mtra. Estefanny Guadarrama Sánchez
Cargo:	Administrador de la bolsa de trabajo
Funciones:	• Consulta de aspirantes y cambio el estatus de CVU, • Consulta de empresas. • Modificar el estatus de ofertas de trabajo publicadas. • Generar los reportes de las ofertas publicadas.
Obligaciones:	• Mantener confidencialidad de los datos de las empresas registradas. • Mantener confidencialidad de los datos de los aspirantes y CVU publicadas.

(Nombre del Usuario 2)	Aspirante (Múltiples usuarios se registran como reclutadores de empresas).
Cargo:	Aspirante (Alumnos)
Funciones:	Registro de datos y del CVU.
Obligaciones:	Mantener actualizada la información.
(Nombre del Usuario 3)	Reclutador (Múltiples usuarios se registran como reclutadores de empresas).
Cargo:	Reclutador (Responsable de la empresa reclutadora)
Funciones:	Registro y actualización de los datos de empresa, puesto y cargo, así como la publicación de las ofertas de trabajo y fechas de vigencia.
Obligaciones:	Mantener actualizada la información de la empresa y de las ofertas de trabajo.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIBT01**
(Nombre del sistema A7)	Sistema de información de bolsa de trabajo
Tipo de soporte:	El soporte es electrónico y vía telefónica.
Descripción:	Base de datos relacional
Características del lugar donde se resguardan los soportes:	Sitio dentro del Centro de Informática de la FCA ubicado en la planta baja, cuenta con aire acondicionado a 18° centígrados, el acceso es con puerta de marco laminado y con vidrio, cuenta con una cerradura sencilla, la llave y la copia es manejada por el Administrador de Servidores y el jefe del Centro de Informática.

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIBT01	
(Nombre del sistema A7)	Sistema de información de bolsa de trabajo	
Riesgo *Describa el riesgo. Agregue un renglón para cada uno*	**Impacto** *Describa el impacto que el riesgo implica para los datos personales*	**Mitigación** *Describa las medidas para mitigación del riesgo y su impacto los datos personales.*

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

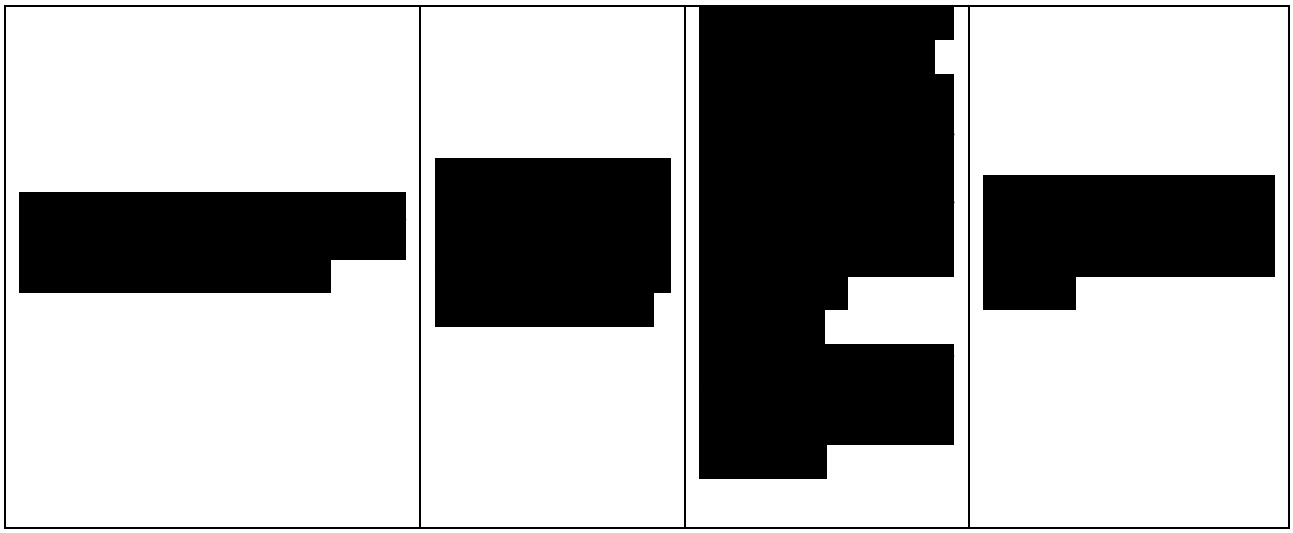
ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIBT01	
(Nombre del sistema A7)	Sistema de información de bolsa de trabajo	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIBT01		
(Nombre del sistema A7)	Sistema de información de bolsa de trabajo		
Actividad	**Descripción**	**Duración**	**Cobertura**

[22] **Texto eliminado:** Apartado correspondiente a “Análisis de Riesgos, de Análisis de Brecha y del Plan de Trabajo” (páginas 69 a 70). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.



MEDIDAS DE SEGURIDAD IMPLEMENTADAS

TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIBT01
(Nombre del sistema A7)	Sistema de información de bolsa de trabajo
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica, no se reciben documentos o expedientes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No aplica, no se intercambian archivos electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de la información es por medio de una red pública y se considera posteriormente se incluirá una red privada virtual (VPN).

RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Nombre	Cargo	Funciones	Obligaciones
Mtro. Balfred Santaella Hinojosa	Jefe del Centro de Informática	Planeación, organización y control de los sistemas de	Asegurar el funcionamiento de los

[23] **Texto eliminado:** Apartado correspondiente a “Plan de Trabajo” (página 70). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

		información de la Facultad.	sistemas y servicios de información.
Mtro. Germán Ignacio Cervantes González	Administrador de Servidores	Gestión, configuración, mantenimiento y soporte de los servidores y las bases de datos.	Revisar y mantener la correcta operación y disponibilidad de los servicios que dan soporte a los distintos sistemas de información.

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado.

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales.

PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

y) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
No
z) ¿Es discrecional (matriz de control de acceso)?
No
aa) ¿Está basado en roles (perfiles) o grupos?
Sí
bb) ¿Está basado en reglas?
No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
s) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
t) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
u) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento

de datos personales:

m) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
No

n) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:

s) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema

t) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema

u) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:

s) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

t) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí

u) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

25. Señalar si realiza respaldos

s) Completos_X_, diferenciales ___ o incrementales___;

t) De forma automática ____ o Manual __X___,

u) Periodicidad con que los realiza: ___semanal____

26. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
Discos duros

27. Cómo y dónde archiva esos medios, y
Arreglos de discos

28. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
Administrador de servidores

PLAN DE CONTINGENCIA

No se cuenta con plan de contingencia, pero se planea desarrollarlo

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIBT01	
(Nombre del sistema A7)	Sistema de información de Bolsa de Trabajo	
Recurso	**Descripción**	**Control**
NANGIOS	Monitorea los recursos y servicios de los servidores.	Lo lleva a cabo el administrador de servidores Licencias de software libre

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIBT01	
(Nombre del sistema A7)	Sistema de información de Bolsa de Trabajo	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIBT01	
(Nombre del sistema A7)	Sistema de información de bolsa de trabajo	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIBT01		
(Nombre del sistema A7)	Sistema de información de Bolsa de Trabajo		
Actividad	**Descripción**	**Duración**	**Cobertura**
La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIBT01		
(Nombre del sistema A7)	Sistema de información de Bolsa de Trabajo		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir el enlace al aviso de privacidad	Se realiza de manera electrónica	Permanente	Usuarios del sistema

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIBT01

(Nombre del sistema A7)	Sistema de información de bolsa de trabajo		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso de privacidad vigente*	*Permanente*	*Usuarios del sistema*

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIBT01		
(Nombre del sistema A7)	Sistema de información de bolsa de trabajo		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	Se descargan e instalan de manera manual	Cada que se recibe notificación de un nuevo parche de seguridad	Mantener la integridad de los datos ante amenazas
Limpieza de logs	Se elimina información histórica de bitácoras	Mensual	Ayuda a liberar espacio de almacenamiento

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIBT01	
(Nombre del sistema A7)	Sistema de información de bolsa de trabajo	
Proceso	**Descripción**	**Responsable**

Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes* *Copiar un nuevo respaldo*	*Administrador de servidores* *Mtro. Germán Ignacio Cervantes González*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIBT01	
(Nombre del sistema A7)	Sistema de información de bolsa de trabajo	
Proceso	**Descripción**	**Responsable**
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	Administrador de servidores *Mtro. Germán Ignacio Cervantes González*

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A8 SISTEMA DE INFORMACIÓN DE ADMISIÓN AL POSGRADO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASISAP01**
Nombre del Sistema A8):	Sistema de información de admisión al posgrado
Datos personales contenidos en el sistema:	Datos de identificación. De aspirantes: Nacionalidad, nombre, apellido paterno, apellido materno, correo, teléfono domicilio, teléfono celular, calle, colonia, código postal, estado, delegación o municipio.
Responsable:	

Nombre:	**Mtro. Balfred Santaella Hinojosa**
Cargo:	**Jefe del Centro de Informática**
Funciones:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1)	**Mtro. Hugo Díaz García**
Cargo:	Jefe de Sistemas
Funciones:	Soporte al área para la automatización de datos personales de aspirantes al proceso de admisión para el estudio de un grado académico. Manejo de la base de datos.
Obligaciones:	Almacenamiento e integridad de la información. Emplear los datos personales dentro el proceso definido y para los fines del sistema.
	Usuarios:
(Nombre del Usuario 1)	Mtra. María Eugenia Patiño Navarro
Cargo:	Administrador de admisión a posgrado
Funciones:	Consulta de aspirante, validar inscripción al proceso de admisión, generación y publicación de resultados.
Obligaciones:	Mantener confidencialidad de los datos de los aspirantes inscritos. Generar y publicar los resultados de admisión, mostrando solo el nombre del aspirante.
(Nombre del Usuario 2)	Aspirante
Cargo:	Aspirante (Alumnos) (Múltiples usuarios que se registran en el proceso de admisión actual o de anteriores).
Funciones:	Registro de datos generales, domicilio, comunicación, nivel(es) escolar(es) y selección del grado académico de estudios de posgrado que aspira a ingresar.
Obligaciones:	Registrar y validar el registro al proceso de admisión al programa seleccionado.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

(Denominación del área específica del Área Universitaria A)* División de Estudios de Posgrado	
Identificador único	**FCASISAP01**
(Nombre del sistema A8)	Sistema de información de admisión al posgrado
Tipo de soporte:	El soporte es electrónico y vía telefónica.
Descripción:	Base de datos relacional

Características del lugar donde se resguardan los soportes:	Sitio dentro del Centro de Informática de la FCA ubicado en la planta baja, cuenta con aire acondicionado a 18° centígrados, el acceso es con puerta de marco laminado y con vidrio, cuenta con una cerradura sencilla, la llave y la copia es manejada por el Administrador de Servidores y el jefe del Centro de Informática.

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASISAP01	
(Nombre del sistema A8)	Sistema de información de admisión al posgrado	
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASISAP01	
(Nombre del sistema A8)	Sistema de información de admisión al posgrado	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**

[24] **Texto eliminado:** Apartado correspondiente a "Análisis de Riesgos y de Análisis de Brecha" (páginas 78 a 79). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASISAP01		
(Nombre del sistema A8)	Sistema de información de admisión al posgrado		
Actividad	**Descripción**	**Duración**	**Cobertura**
[redacted]	[redacted]	[redacted]	[redacted]

MEDIDAS DE SEGURIDAD IMPLEMENTADAS

TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASISAP01
(Nombre del sistema A)	Sistema de información de admisión al posgrado.
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica, no se reciben documentos o expedientes físicos.

[25] **Texto eliminado:** Apartado correspondiente a "Análisis de Brecha y del Plan de Trabajo" (página 79). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Transferencias mediante el traslado de soportes electrónicos:	No aplica, no se intercambian archivos electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de la información es por medio de una red pública y se considera posteriormente incluirá una red privada virtual (VPN).

RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Nombre	Cargo	Funciones	Obligaciones
Mtro. Balfred Santaella Hinojosa	Jefe del Centro de Informática	Planeación, organización y control de los sistemas de información de la Facultad.	Asegurar el funcionamiento de los sistemas y servicios de información.
Mtro. Germán Ignacio Cervantes González	Administrador de Servidores	Gestión, configuración, mantenimiento y soporte de los servidores y las bases de datos.	Revisar y mantener la correcta operación y disponibilidad de los servicios que dan soporte a los distintos sistemas de información.

BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**

   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   No se registran bitácoras en el sistema, se emplean los logs del servidor.

   b) Para soportes físicos: Número o clave del expediente utilizado, y
   No aplica.

   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
   No aplica.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
   Los logs del servidor como soporte electrónico.
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
   En el sistema operativo de red de manera semanal.
4. La manera en que asegura la integridad de las bitácoras, y
   Con respaldos semanales.
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada

cuándo las analiza, y
Administrador de servidores.
b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
No hay herramientas de análisis.

REGISTRO DE INCIDENTES

1. Los datos que registra:
a) La persona que resolvió el incidente;
Germán Ignacio Cervantes Gonzáles (Servidores) y/o Hugo Díaz García (Responsable del sistema)
b) La metodología aplicada;

- **i.** Se genera un informe con los daños ocurridos y el equipo faltante en el centro de datos, a partir de que se pueda acceder a las instalaciones se genera una lista de los servidores dañados junto con los sistemas que se ven afectados y el inventario del equipo.
- **ii.** Del incidente se toman fotografías y se genera un acta por el o la abogad(a) de la facultad con el fin de denunciar los hechos ante el ministerio público, se informará al abogado general de UNAM y autoridades universitarias acerca de las afectaciones.
- **iii.** Durante no más a 5 días naturales de ocurrido el incidente se hace pública la denuncia y es publicada en la página de la FCA informando a la comunidad de los hechos, así como del robo y/o daño de la información sustraída.
- **iv.** En el caso de robo de datos personales se alertará a los titulares por medio de un correo masivo del evento para que tomen sus precauciones acerca del uso indebido de los datos personales.
- **v.** En el caso de un ataque externo se le informa del incidente a la DGTIC para que se tomen medidas correctivas y precautorias.

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.
Del incidente se revisa el servidor y los respaldos para conocer que se puede recuperar y que se debe reinstalar y restaurar.
2. Si el registro está en soporte físico o en soporte electrónico;
El registro está en soporte electrónico.
3. Cómo asegura la integridad de dicho registro, y
Empleando un MD5 y revisando los últimos índices de las principales tablas.
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.
Mtro. Balfred Santaella Hinojosa (Jefe del Centro de Informática)

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado.

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales.

PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
No
b) ¿Es discrecional (matriz de control de acceso)?
No
c) ¿Está basado en roles (perfiles) o grupos?
Sí
d) ¿Está basado en reglas?
No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
No
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema
b) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema
c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí
c) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   v) Completos_ X _, diferenciales ___ o incrementales___;
   w) De forma automática ____ o Manual __X___,
   x) Periodicidad con que los realiza: ___semanal____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Discos duros
3. Cómo y dónde archiva esos medios, y
   Arreglos de discos
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Administrador de servidores.

PLAN DE CONTINGENCIA

No se cuenta con plan de contingencia, pero se planea desarrollarlo

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAP01	
(Nombre del sistema A8)	Sistema de información de admisión al posgrado	
Recurso	**Descripción**	**Control**
NANGIOS	Monitorea los recursos y servicios de los servidores.	Lo lleva a cabo el administrador de servidores Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)

Identificador único	FCASISAP01	
(Nombre del sistema A8)	Sistema de información de admisión al posgrado	
Medida de seguridad*	**Procedimiento***	**Responsable***
No aplica.	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASISAP01	
(Nombre del sistema A8)	Sistema de información de admisión al posgrado	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASISAP01	
(Nombre del sistema A8)	Sistema de información de admisión al posgrado	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASISAP01		
(Nombre del sistema A8)	Sistema de información de admisión al posgrado		
Actividad	**Descripción**	**Duración**	**Cobertura**
La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASISAP01		
(Nombre del sistema A8)	Sistema de información de admisión al posgrado		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir el enlace al aviso de privacidad	Se realiza de manera electrónica	Permanente	Usuarios del sistema

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASISAP01

(Nombre del sistema A8)	Sistema de información de admisión al posgrado		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso de privacidad vigente*	*Permanente*	*Usuarios del sistema*

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASISAP01		
(Nombre del sistema A8)	Sistema de información de admisión al posgrado		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	Se descargan e instalan de manera manual	Cada que se recibe notificación de un nuevo parche de seguridad	Mantener la integridad de los datos ante amenazas
Limpieza de logs	Se elimina información histórica de bitácoras	Mensual	Ayuda a liberar espacio de almacenamiento

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASISAP01
(Nombre del sistema A8)	Sistema de información de admisión al posgrado

Proceso	Descripción	Responsable
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes* *Copiar un nuevo respaldo*	*Administrador de servidores* *Mtro. Germán Ignacio Cervantes González*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASISAP01	
(Nombre del sistema A8)	Sistema de información de admisión al posgrado	
Proceso*	**Descripción***	**Responsable***
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	Administrador de servidores *Mtro. Germán Ignacio Cervantes González*

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A9 SISTEMA DE INFORMACIÓN DEL CONGRESO DE INVESTIGACIÓN

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASICI01**
Sistema (Nombre del A9):	Sistema de información del congreso de investigación
Datos personales contenidos en el sistema:	Datos de identificación.

	Participante: Nombre, apellido paterno, apellido materno, institución de procedencia, correo, teléfono.
Responsable:	
Nombre:	**Mtro. Balfred Santaella Hinojosa**
Cargo:	**Jefe del Centro de Informática**
Funciones:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1)	**Mtro. Hugo Díaz García**
Cargo:	Jefe de Sistemas
Funciones:	Soporte al área para el registro de datos personales de participantes al congreso de investigación. Manejo de la base de datos.
Obligaciones:	Almacenamiento e integridad de la información. Emplear los datos personales dentro el proceso definido y para los fines del sistema.
	Usuarios:
(Nombre del Usuario 1)	Mtro. José Silvestre Méndez Morales Mtro. José Luis Arias Negrete
Cargo:	Administrador del congreso de investigación
Funciones:	• Consulta de datos personales de participantes que se registran al congreso de investigación. • Revisión de trabajos publicados de investigadores y envío de carta de dictamen a los autores por correo. • Generación de reporte de participantes inscritos y trabajos enviados.
Obligaciones:	• Manejo de datos personales para el uso exclusivo de la asistencia de participante general y de autores que envían trabajos para su respectivo arbitraje. • Publicar los trabajos aceptados, con base a la cesión de derechos de los autores, mostrando solamente los nombres de los autores y sus correos, necesarios para la publicación de programa y la memoria del congreso.
(Nombre del Usuario 2)	Inscripción Sofía Margarita Chimal González
Cargo:	Responsable de la inscripción de participantes de forma presencial.
Funciones:	Registro de participantes solicita: el nombre, apellido paterno, apellido materno, institución de procedencia, correo, teléfono.
Obligaciones:	• Registrar a los participantes al congreso de investigación. • Actualizar datos acerca del registro, corrección en

	caso de cambios.
(Nombre del Usuario 3)	Autor (Múltiples usuarios que se registran en el congreso actual o de anteriores).
Cargo:	Publica el trabajo de investigación realizado, el cual posteriormente será sometido a arbitraje.
Funciones:	• Registrarse como participante general. • Registrar el título de trabajo, área de investigación, palabras clave, y archivos de carátula, resumen y contenido, y su folio de registro de participante.
Obligaciones:	Registrar y actualizar el trabajo en caso de observaciones.
(Nombre del Usuario 4)	Arbitro (Múltiples usuarios que se registran en el congreso actual o de anteriores).
Cargo:	Realiza un arbitraje ciego para la evaluación del trabajo.
Funciones:	• Revisa el trabajo a evaluar. • Emite dictamen del trabajo de investigación.
Obligaciones:	Revisa la estructura y contenido del trabajo publicado, y realiza el dictamen del mismo, desconoce el nombre del autor o autores.
(Nombre del Usuario 5)	Contabilidad L.C. Lucero Vázquez Díaz
Cargo:	Responsable del área administrativa
Funciones:	• Consulta de participantes inscritos para obtener el folio de registro. • Revisa por correo el envío de transferencias, depósitos de pago para la asistencia al congreso.
Obligaciones:	• Maneja de forma confidencial el nombre y correo del participante para la gestión de ingresos. • Mantiene la comunicación directa con el participante vía correo o telefónicamente para la emisión de comprobantes.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASICI01**
(Nombre del sistema A9)	Sistema de información del congreso internacional
Tipo de soporte:	El soporte es electrónico y vía telefónica.
Descripción:	Base de datos relacional
Características del lugar donde se resguardan los soportes:	Sitio dentro del Centro de Informática de la FCA ubicado en la planta baja, cuenta con aire acondicionado a 18° centígrados, el acceso es con puerta de marco laminado y con vidrio, cuenta con una cerradura sencilla, la llave y la copia es manejada por el Administrador de Servidores y el jefe del Centro de Informática.

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASICI01	
(Nombre del sistema A9)	Sistema de información del congreso de investigación	
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASICI01	
(Nombre del sistema A9)	Sistema de información del congreso internacional	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

[26] **Texto eliminado:** Apartado correspondiente a “Análisis de Riesgos, de Análisis de Brecha y del Plan de Trabajo” (páginas 90 a 91). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASICI01		
(Nombre del sistema A9)	Sistema de información del congreso de investigación		
Actividad	**Descripción**	**Duración**	**Cobertura**
[redacted]	[redacted]	[redacted]	[redacted]

MEDIDAS DE SEGURIDAD IMPLEMENTADAS

TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASICI01
(Nombre del sistema A9)	Sistema de información del congreso internacional
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica, no se reciben documentos o expedientes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No aplica, no se intercambian archivos electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de la información es por medio de una red pública y se considera posteriormente incluir red privada virtual (VPN).

[27] T**exto eliminado:** Apartado correspondiente a “Plan de Trabajo” (página 91). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Nombre	Cargo	Funciones	Obligaciones
Mtro. Balfred Santaella Hinojosa	Jefe del Centro de Informática	Planeación, organización y control de los sistemas de información de la Facultad.	Asegurar el funcionamiento de los sistemas y servicios de información.
Mtro. Germán Ignacio Cervantes González	Administrador de Servidores	Gestión, configuración, mantenimiento y soporte de los servidores y las bases de datos.	Revisar y mantener la correcta operación y disponibilidad de los servicios que dan soporte a los distintos sistemas de información.

BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**
   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   No se registran bitácoras en el sistema, se emplean los logs del servidor.

   b) Para soportes físicos: Número o clave del expediente utilizado, y
   No aplica.

   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
   No aplica.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
   Los logs del servidor como soporte electrónico.
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
   En el sistema operativo de red de manera semanal.
4. La manera en que asegura la integridad de las bitácoras, y
   Con respaldos semanales.
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
   Administrador de servidores.
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
   No hay herramientas de análisis.

REGISTRO DE INCIDENTES

1. Los datos que registra:

a) La persona que resolvió el incidente;

Germán Ignacio Cervantes Gonzáles (Servidores) y/o Hugo Díaz García (Responsable del sistema)

b) La metodología aplicada;

- **i.** Se genera un informe con los daños ocurridos y el equipo faltante en el centro de datos, a partir de que se pueda acceder a las instalaciones se genera una lista de los servidores dañados junto con los sistemas que se ven afectados y el inventario del equipo.
- **ii.** Del incidente se toman fotografías y se genera un acta por el o la abogad(a) de la facultad con el fin de denunciar los hechos ante el ministerio público, se informará al abogado general de UNAM y autoridades universitarias acerca de las afectaciones.
- **iii.** Durante no más a 5 días naturales de ocurrido el incidente se hace pública la denuncia y es publicada en la página de la FCA informando a la comunidad de los hechos, así como del robo y/o daño de la información sustraída.
- **iv.** En el caso de robo de datos personales se alertará a los titulares por medio de un correo masivo del evento para que tomen sus precauciones acerca del uso indebido de los datos personales.
- **v.** En el caso de un ataque externo se le informa del incidente a la DGTIC para que se tomen medidas correctivas y precautorias.

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y

d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

Del incidente se revisa el servidor y los respaldos para conocer que se puede recuperar y que se debe reinstalar y restaurar.

2. Si el registro está en soporte físico o en soporte electrónico;

El registro esta en soporte electrónico.

3. Cómo asegura la integridad de dicho registro, y

Empleando un MD5 y revisando los últimos índices de las principales tablas.

4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

Mtro. Balfred Santaella Hinojosa (Jefe del Centro de Informática)

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado.

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales.

PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
No
b) ¿Es discrecional (matriz de control de acceso)?
No
c) ¿Está basado en roles (perfiles) o grupos?
Sí
d) ¿Está basado en reglas?
No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
No
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema
b) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema
c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí
c) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_X_, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual __X___,
   c) Periodicidad con que los realiza: ___semanal____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:

Discos duros

3. Cómo y dónde archiva esos medios, y
   Arreglos de discos
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Administrador de servidores

PLAN DE CONTINGENCIA

No se cuenta con plan de contingencia, pero se planea desarrollarlo.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASICI01	
(Nombre del sistema A9)	Sistema de información del congreso internacional	
Recurso	**Descripción**	**Control**
NANGIOS	Monitorea los recursos y servicios de los servidores.	Lo lleva a cabo el administrador de servidores Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASICI01	
(Nombre del sistema A9)	Sistema de información del congreso internacional	
Medida de seguridad	**Procedimiento**	**Responsable**
No aplica.	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASICI01	
(Nombre del sistema A9)	Sistema de información del congreso internacional	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASICI01	
(Nombre del sistema A9)	Sistema de información del congreso internacional	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN
Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASICI01		
(Nombre del sistema A9)	Sistema de información del congreso de investigación		
Actividad	**Descripción**	**Duración**	**Cobertura**

La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASICI01		
(Nombre del sistema A9)	Sistema de información del congreso internacional		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir el enlace al aviso de privacidad	Se realiza de manera electrónica	Permanente	Usuarios del sistema

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASICI01		
(Nombre del sistema A9)	Sistema de información del congreso internacional		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso*	*Permanente*	*Usuarios del sistema*

	de privacidad vigente		

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASICI01		
(Nombre del sistema A9)	Sistema de información del congreso internacional		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	Se descargan e instalan de manera manual	Cada que se recibe notificación de un nuevo parche de seguridad	Mantener la integridad de los datos ante amenazas
Limpieza de logs	Se elimina información histórica de bitácoras	Mensual	Ayuda a liberar espacio de almacenamiento

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASICI01	
(Nombre del sistema A9)	Sistema de información del congreso internacional	
Proceso	**Descripción**	**Responsable**
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes*	*Administrador de servidores* *Mtro. Germán Ignacio Cervantes González*

	Copiar un nuevo respaldo	

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASICI01	
(Nombre del sistema A9)	Sistema de información del congreso de investigación	
Proceso	**Descripción**	**Responsable**
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	Administrador de servidores *Mtro. Germán Ignacio Cervantes González*

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A10 SISTEMA DE INFORMACIÓN DE ASIGNACIÓN DE PROFESORES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIAP01**
Sistema (Nombre del A10):	Sistema de información de asignación de profesores
Datos personales contenidos en el sistema:	Datos de identificación. De profesores: Nombre, apellido paterno, apellido materno, RFC, CURP y número de trabajador UNAM.
Responsable:	
Nombre:	**Mtro. Balfred Santaella Hinojosa**
Cargo:	**Jefe del Centro de Informática**

Funciones:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1*)	**Mtro. Hugo Díaz García**
Cargo:	Jefe de Sistemas
Funciones:	Soporte al área para la gestión de registro y asignación de profesores a grupo para la conformación de la plantilla de cada semestre por parte de los coordinadores académicos. Manejo de la base de datos.
Obligaciones:	Almacenamiento e integridad de la información. Emplear los datos personales dentro el proceso definido y para los fines del sistema.
	Usuarios:
(Nombre del Usuario 1)	Mtro. Gustavo Almaguer Pérez Mtro. Jesús Mata Pacheco
Cargo:	Administrador de movimientos y prestaciones
Funciones:	• Alta, consulta y actualización de datos de profesores. • Consulta de la plantilla de profesores de grupos ordinarios y extraordinarios. • Comunicación con profesores para recepción de documentación pendiente.
Obligaciones:	• Mantener la confidencialidad de los datos de profesores para la generación o cancelación de contratos. • Emplear la información para tramites como licencias e incapacidades del profesor.
(Nombre del Usuario 2)	**Jefe de División** Alfonso Ayala Rico Rosa Martha Barona Peña Silvia Berenice Villamil Rodríguez María del Rocío Huitrón Hernández Marlene Olga Ramírez Chavero **Coordinador de licenciatura** Alfonso Manuel Aguilar Guevara María Gloria Arévalo Guerrero Eva Elizabeth del Valle Córdova Graciela Enríquez Guadarrama Gabriel Guevara Gutiérrez Javier Isaac Osorio González Francisco Alberto Piña Salazar Pedro Eduardo Quezada García María Angélica Alicia Raya Sánchez Isaías Reyes Bojórquez Carlos Ruiz Díaz Carlos Ríos Murillo Alma Lucero Sosa Blancas Karen Gisel Velázquez Rojas

	Israel Vladimir Villa García Romeo Vite López **Coordinador de posgrado** Alfredo Corona Cabrera Scott Michel Martín Da Gama Darby Silvia Adriana Durand Bautista M. Cristina García García Francisco Gerardo Serrano Luis Alberto Gómez Alvarado María del Rosario Higuera Torres María Eugenia Miranda Jaimes María Amalia Belén Negrete Vargas José Padilla Hernández **Coordinador del SUAyED** Martha Patricia García Chavero Sara Guadalupe Espinosa de los Monteros Montes de Oca
Cargo:	Jefe de División, Coordinador académico de licenciatura, Coordinador académico de posgrado, Coordinador del SUAyED.
Funciones:	Consulta de profesores para la asignación a grupo. Generación de la plantilla de la coordinación.
Obligaciones:	Mantener confidencial la información del profesor empleada en la asignación del mismo a grupo y para la conformación de la plantilla semestral. Notificar al profesor de la asignación de grupo.
(Nombre del Usuario 3)	**Movimientos y Prestaciones** Mónica Elizabeth Espejel Hernández Rocío Pérez de León Vargas Carla Renata Rosas Moreno Beatriz Adriana Flores Muñoz
Cargo:	Coordinador de Movimientos y Prestaciones
Funciones:	• Registro y actualización de profesores. • Generación de los contratos por medio de la consulta de la plantilla.
Obligaciones:	• Mantener actualizada y confidencialidad de los datos de profesor y de los grupos asignados.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIAP01**
(Nombre del sistema A10)	Sistema de información de asignación de profesores
Tipo de soporte:	El soporte es electrónico y vía telefónica.
Descripción:	Base de datos relacional

Características del lugar donde se resguardan los soportes:	Sitio dentro del Centro de Informática de la FCA ubicado en la planta baja, cuenta con aire acondicionado a 18° centígrados, el acceso es con puerta de marco laminado y con vidrio, cuenta con una cerradura sencilla, la llave y la copia es manejada por el Administrador de Servidores y el jefe del Centro de Informática.

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAP01	
(Nombre del sistema A10)	Sistema de información de asignación de profesores	
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAP01	
(Nombre del sistema A10)	Sistema de información de asignación de profesores	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**

[28] T**exto eliminado:** Apartado correspondiente a “Análisis de Riesgos y de Análisis de Brecha” (páginas 102 a 103). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIAP01		
(Nombre del sistema A10)	Sistema de información de asignación de profesores		
Actividad	**Descripción**	**Duración**	**Cobertura**
[redacted]	[redacted]	[redacted]	[redacted]

MEDIDAS DE SEGURIDAD IMPLEMENTADAS
TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIAP01
(Nombre del sistema A10)	Sistema de información de asignación de profesores
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica, no se reciben documentos o expedientes físicos.

[29] **Texto eliminado:** Apartado correspondiente a "Análisis de Brecha y del Plan de Trabajo" (página 103). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Transferencias mediante el traslado de soportes electrónicos:	No aplica, no se intercambian archivos electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de la información es por medio de una red pública y se considera posteriormente incluir red privada virtual (VPN).

RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Nombre	Cargo	Funciones	Obligaciones
Mtro. Balfred Santaella Hinojosa	Jefe del Centro de Informática	Planeación, organización y control de los sistemas de información de la Facultad.	Asegurar el funcionamiento de los sistemas y servicios de información.
Mtro. Germán Ignacio Cervantes González	Administrador de Servidores	Gestión, configuración, mantenimiento y soporte de los servidores y las bases de datos.	Revisar y mantener la correcta operación y disponibilidad de los servicios que dan soporte a los distintos sistemas de información.

BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**

   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   No se registran bitácoras en el sistema, se emplean los logs del servidor.

   b) Para soportes físicos: Número o clave del expediente utilizado, y
   No aplica.

   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
   No aplica.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
   Los logs del servidor como soporte electrónico.
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
   En el sistema operativo de red de manera semanal.
4. La manera en que asegura la integridad de las bitácoras, y
   Con respaldos semanales.
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
   Administrador de servidores.

b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

No hay herramientas de análisis.

REGISTRO DE INCIDENTES

1. Los datos que registra:

a) La persona que resolvió el incidente;

Germán Ignacio Cervantes Gonzáles (Servidores) y/o Hugo Díaz García (Responsable del sistema)

b) La metodología aplicada;

- **i.** Se genera un informe con los daños ocurridos y el equipo faltante en el centro de datos, a partir de que se pueda acceder a las instalaciones se genera una lista de los servidores dañados junto con los sistemas que se ven afectados y el inventario del equipo.
- **ii.** Del incidente se toman fotografías y se genera un acta por el o la abogad(a) de la facultad con el fin de denunciar los hechos ante el ministerio público, se informará al abogado general de UNAM y autoridades universitarias acerca de las afectaciones.
- **iii.** Durante no más a 5 días naturales de ocurrido el incidente se hace pública la denuncia y es publicada en la página de la FCA informando a la comunidad de los hechos, así como del robo y/o daño de la información sustraída.
- **iv.** En el caso de robo de datos personales se alertará a los titulares por medio de un correo masivo del evento para que tomen sus precauciones acerca del uso indebido de los datos personales.
- **v.** En el caso de un ataque externo se le informa del incidente a la DGTIC para que se tomen medidas correctivas y precautorias.

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y

d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

Del incidente se revisa el servidor y los respaldos para conocer que se puede recuperar y que se debe reinstalar y restaurar.

2. Si el registro está en soporte físico o en soporte electrónico;

El registro está en soporte electrónico.

3. Cómo asegura la integridad de dicho registro, y

Empleando un MD5 y revisando los últimos índices de las principales tablas.

4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

Mtro. Balfred Santaella Hinojosa (Jefe del Centro de Informática)

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado.

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales.

PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
No
b) ¿Es discrecional (matriz de control de acceso)?
No
c) ¿Está basado en roles (perfiles) o grupos?
Sí
d) ¿Está basado en reglas?
No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
No
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema
b) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema
c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí
c) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

d) Completos_X_, diferenciales ___ o incrementales___;
e) De forma automática ____ o Manual __X___,
f) Periodicidad con que los realiza: ___semanal____

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Discos duros
3. Cómo y dónde archiva esos medios, y
   Arreglos de discos
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Administrador de servidores

PLAN DE CONTINGENCIA

No se cuenta con plan de contingencia, pero se planea desarrollarlo.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAP01	
(Nombre del sistema A10)	Sistema de información de asignación de profesor	
Recurso	**Descripción**	**Control**
NANGIOS	Monitorea los recursos y servicios de los servidores.	Lo lleva a cabo el administrador de servidores Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIAP01

(Nombre del sistema A10)	Sistema de información de asignación de profesores	
Medida de seguridad	**Procedimiento**	**Responsable**
No aplica.	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAP01	
(Nombre del sistema A10)	Sistema de información de asignación de profesores	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAP01	
(Nombre del sistema A10)	Sistema de información de asignación de profesores	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIAP01		
(Nombre del sistema A10)	Sistema de información de asignación de profesores		
Actividad	**Descripción**	**Duración**	**Cobertura**
La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIAP01		
(Nombre del sistema A10)	Sistema de información de asignación de profesores		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir el enlace al aviso de privacidad	Se realiza de manera electrónica	Permanente	Usuarios del sistema

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIAP01		
(Nombre del sistema A10)	Sistema de información de asignación de profesores		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso de privacidad vigente*	*Permanente*	*Usuarios del sistema*

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIAP01		
(Nombre del sistema A10)	Sistema de información de asignación de profesores		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	Se descargan e instalan de manera manual	Cada que se recibe notificación de un nuevo parche de seguridad	Mantener la integridad de los datos ante amenazas
Limpieza de logs	Se elimina información histórica de bitácoras	Mensual	Ayuda a liberar espacio de almacenamiento

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAP01	
(Nombre del sistema A10)	Sistema de información de asignación de profesores	
Proceso	**Descripción**	**Responsable**
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes* *Copiar un nuevo respaldo*	*Administrador de servidores* *Mtro. Germán Ignacio Cervantes González*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAP01	
(Nombre del sistema A10)	Sistema de información de asignación de profesores	
Proceso	**Descripción**	**Responsable**
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	Administrador de servidores *Mtro. Germán Ignacio Cervantes González*

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A11 SISTEMA DE INFORMACIÓN DE EXÁMENES PROFESIONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIEP01**
Sistema (Nombre del A11):	Sistema de información de exámenes profesionales
Datos personales contenidos en el sistema:	Datos de identificación. De alumnos: número de cuenta, fecha de nacimiento, universidad, plantel, carrera, sistema, promedio, apellido paterno, apellido materno, nombre, sexo, nacionalidad, CURP, domicilio (estado, calle, no. exterior, no. Interior, código postal, colonia, delegación/municipio), teléfono particular, celular, oficina y correo electrónico.
Responsable:	
Nombre:	**Mtro. Balfred Santaella Hinojosa**
Cargo:	**Jefe del Centro de Informática**
Funciones:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1)	**Mtro. Hugo Díaz García**
Cargo:	Jefe de Sistemas
Funciones:	Soporte al área para la gestión del registro de alumnos que desean cursar alguna de las opciones de titulación. Manejo de la base de datos.
Obligaciones:	Almacenamiento e integridad de la información. Emplear los datos personales dentro el proceso definido y para los fines del sistema.
	Usuarios:
(Nombre del Usuario 1)	**Mtra. Norma Angélica González Buendía**
Cargo:	Administrador de exámenes profesionales
Funciones:	• Manejo de datos personales de alumnos para el proceso de inscripción a alguna opción de titulación. • Revisión y validación de documentación para el proceso de inscripción y de titulación. • Comunicación con alumnos para el trámite de titulación y programación de examen de licenciatura.
Obligaciones:	• Manejo adecuado y confidencial de datos personales para el uso exclusivo del proceso de la opción de titulación. • Expedición de constancias a los alumnos que cursan alguna opción de titulación. • Generación de reportes de alumnos inscritos de acuerdo a la opción de titulación.

(Nombre del Usuario 2)	Coordinadora Dra. Dorín Cecilia Flores Mondragón Dra. Brigitte Hayde Treviño Hernández Mtra. María Virginia Negrete Martínez Mtra. Martha Santiago García
Cargo:	Coordinador de opción de titulación
Funciones:	• Consulta de solicitudes de alumnos. • Inscripción de alumnos a alguna opción de titulación. • Asignación de profesores a grupo de seminario o diplomado o como tutores de tesis. • Generación de constancia de curso a opción de titulación.
Obligaciones:	• Validar y mantener confidencialidad de los datos de alumnos desde el proceso de registro hasta la titulación. • Validar y mantener confidencialidad de los datos de profesores asignados a diplomados y seminarios o como tutores de tesis.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIEP01**
(Nombre del sistema A11)	Sistema de información de exámenes de profesionales
Tipo de soporte:	El soporte es electrónico y vía telefónica.
Descripción:	Base de datos relacional
Características del lugar donde se resguardan los soportes:	Sitio dentro del Centro de Informática de la FCA ubicado en la planta baja, cuenta con aire acondicionado a 18° centígrados, el acceso es con puerta de marco laminado y con vidrio, cuenta con una cerradura sencilla, la llave y la copia es manejada por el Administrador de Servidores y el jefe del Centro de Informática.

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIEP01	
(Nombre del sistema A11)	Sistema de información de exámenes de profesionales	
Riesgo	**Impacto**	**Mitigación**

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

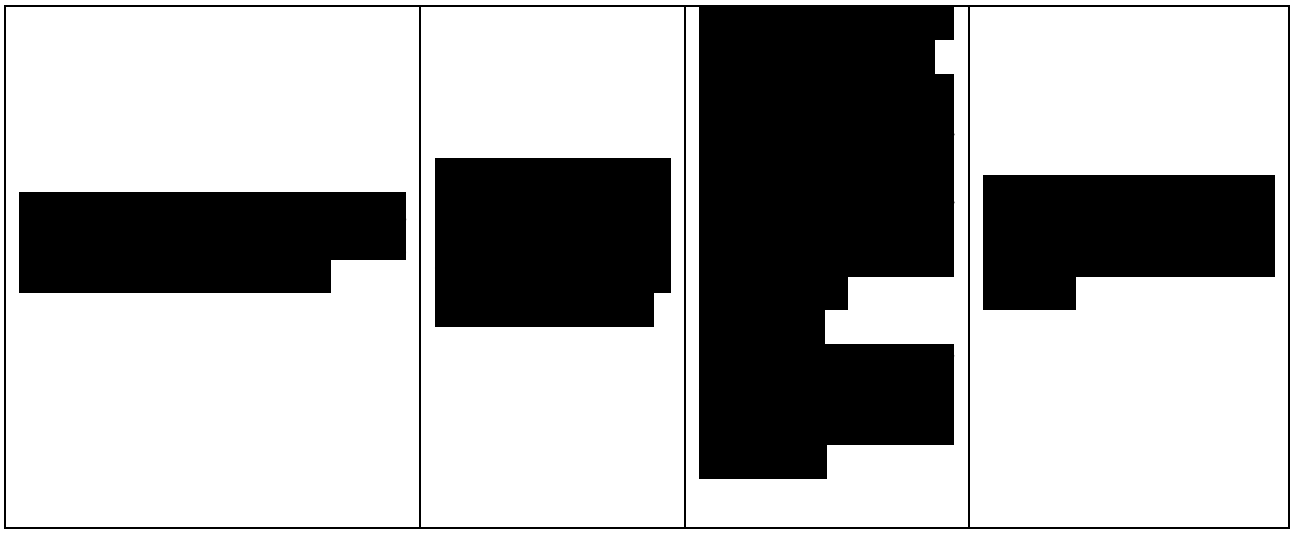
ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIEP01	
(Nombre del sistema A11)	Sistema de información de exámenes de profesionales	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIEP01		
(Nombre del sistema A11)	Sistema de información de exámenes de profesionales		
Actividad	**Descripción**	**Duración**	**Cobertura**

[30] T**exto eliminado:** Apartado correspondiente a “Análisis de Riesgos, de Análisis de Brecha y del Plan de Trabajo” (páginas 114 a 115). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.



MEDIDAS DE SEGURIDAD IMPLEMENTADAS

TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIEP01
(Nombre del sistema A11)	Sistema de información de exámenes profesionales
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica, no se reciben documentos o expedientes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No aplica, no se intercambian archivos electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de la información es por medio de una red pública y se considera posteriormente incluir red privada virtual (VPN).

RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El acceso al centro de datos y servidores es con llave y la chapa es sencilla, existe equipo de refrigeración que mantiene la temperatura a 18°, no existe un mecanismo para detección o supresión de incendios y cuenta con planta de luz y UPS.

Nombre	**Cargo**	**Funciones**	**Obligaciones**
Mtro. Balfred Santaella Hinojosa	Jefe del Centro de Informática	Planeación, organización y control de los sistemas de	Asegurar el funcionamiento de los sistemas y servicios de información.

[32] T**exto eliminado:** Apartado correspondiente a “Plan de Trabajo” (página 115). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

		información de la Facultad.	
Mtro. Germán Ignacio Cervantes González	Administrador de Servidores	Gestión, configuración, mantenimiento y soporte de los servidores y las bases de datos.	Revisar y mantener la correcta operación y disponibilidad de los servicios que dan soporte a los distintos sistemas de información.

BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
No se registran bitácoras en el sistema, se emplean los logs del servidor.

b) Para soportes físicos: Número o clave del expediente utilizado, y
No aplica.

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
No aplica.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
Los logs del servidor como soporte electrónico.
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
En el sistema operativo de red de manera semanal.
4. La manera en que asegura la integridad de las bitácoras, y
Con respaldos semanales.
5. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
Administrador de servidores.

b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
No hay herramientas de análisis.

REGISTRO DE INCIDENTES

1. Los datos que registra:

a) La persona que resolvió el incidente;
Germán Ignacio Cervantes Gonzáles (Servidores) y/o Hugo Díaz García (Responsable del sistema)

b) La metodología aplicada;

- **i.** Se genera un informe con los daños ocurridos y el equipo faltante en el centro de datos, a partir de que se pueda acceder a las instalaciones se genera una lista de los servidores dañados junto con los sistemas que se ven afectados y el inventario del equipo.
- **ii.** Del incidente se toman fotografías y se genera un acta por el o la abogad(a) de la facultad con el fin de denunciar los hechos ante el ministerio público, se informará al

abogado general de UNAM y autoridades universitarias acerca de las afectaciones.

iii. Durante no más a 5 días naturales de ocurrido el incidente se hace pública la denuncia y es publicada en la página de la FCA informando a la comunidad de los hechos, así como del robo y/o daño de la información sustraída.

iv. En el caso de robo de datos personales se alertará a los titulares por medio de un correo masivo del evento para que tomen sus precauciones acerca del uso indebido de los datos personales.

v. En el caso de un ataque externo se le informa del incidente a la DGTIC para que se tomen medidas correctivas y precautorias.

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y

d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

Del incidente se revisa el servidor y los respaldos para conocer que se puede recuperar y que se debe reinstalar y restaurar.

2. Si el registro está en soporte físico o en soporte electrónico;
El registro está en soporte electrónico.

3. Cómo asegura la integridad de dicho registro, y
Empleando un MD5 y revisando los últimos índices de las principales tablas.

4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.
Mtro. Balfred Santaella Hinojosa (Jefe del Centro de Informática)

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado.

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales.

PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
No

b) ¿Es discrecional (matriz de control de acceso)?
No

c) ¿Está basado en roles (perfiles) o grupos?
Sí

d) ¿Está basado en reglas?
No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
No
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema
b) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema
c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí
c) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_X_, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual __X___,
   c) Periodicidad con que los realiza: ___semanal____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Discos duros
3. Cómo y dónde archiva esos medios, y
   Arreglos de discos
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Administrador de servidores

PLAN DE CONTINGENCIA

No se cuenta con plan de contingencia, pero se planea desarrollarlo.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIEP01	
(Nombre del sistema A11)	Sistema de información de exámenes de profesionales	
Recurso	**Descripción**	**Control**
NANGIOS	Monitorea los recursos y servicios de los servidores.	Lo lleva a cabo el administrador de servidores Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIEP01	
(Nombre del sistema A11)	Sistema de información de exámenes de profesionales	
Medida de seguridad	**Procedimiento**	**Responsable**
No aplica.	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIEP01	
(Nombre del sistema A11)	Sistema de información de exámenes de profesionales	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIEP01	
(Nombre del sistema A11)	Sistema de información de exámenes de profesionales	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIEP01		
(Nombre del sistema A11)	Sistema de información de exámenes profesionales		
Actividad	**Descripción**	**Duración**	**Cobertura**

La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIEP01		
(Nombre del sistema A11)	Sistema de información de exámenes de profesionales		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir el enlace al aviso de privacidad	Se realiza de manera electrónica	Permanente	Usuarios del sistema

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIEP01		
(Nombre del sistema A11)	Sistema de información de exámenes de profesionales		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso*	*Permanente*	*Usuarios del sistema*

	de privacidad vigente		

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIEP01		
(Nombre del sistema A11)	Sistema de información de exámenes de profesionales		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	Se descargan e instalan de manera manual	Cada que se recibe notificación de un nuevo parche de seguridad	Mantener la integridad de los datos ante amenazas
Limpieza de logs	Se elimina información histórica de bitácoras	Mensual	Ayuda a liberar espacio de almacenamiento

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIEP01	
(Nombre del sistema A11)	Sistema de información de exámenes de profesionales	
Proceso	**Descripción**	**Responsable**
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos*	*Administrador de servidores* *Mtro. Germán Ignacio Cervantes González*

	Se rotan los respaldos previos para dar entrada a los siguientes *Copiar un nuevo respaldo*	

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIEP01	
(Nombre del sistema A11)	Sistema de información de exámenes profesionales	
Proceso	**Descripción**	**Responsable**
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	Administrador de servidores *Mtro. Germán Ignacio Cervantes González*

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A12 SISTEMA DE INFORMACIÓN DE PROYECTO E INFORME DE ACTIVIDADES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIPIAD01**
Sistema (Nombre del A12):	Sistema de información de proyecto e informe de actividades
Datos personales contenidos en el sistema:	Datos de identificación. De profesores: Nombre, apellido paterno, apellido materno y correo electrónico, RFC y número de empleado UNAM.
Responsable:	
Nombre:	**Mtro. Balfred Santaella Hinojosa**
Cargo:	**Jefe del Centro de Informática**

Funciones:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1)	**Mtro. Hugo Díaz García**
Cargo:	Jefe de Sistemas
Funciones:	Soporte al área para la captura del plan de trabajo de los profesores de las asignaturas que van a impartir clase. Manejo de la base de datos.
Obligaciones:	Almacenamiento e integridad de la información. Emplear los datos personales dentro el proceso definido y para los fines del sistema.
	Usuarios:
(Nombre del Usuario 1)	**Mtra. Beatriz Adriana Flores Muñoz**
Cargo:	Jefa del Departamento de Control Docente y Programas Institucionales
Funciones:	Consulta de los planes de trabajo e informe de los profesores.
Obligaciones:	Manejo adecuado y confidencial de los nombres de los profesores para el uso exclusivo de la evaluación al Programa de Estímulos a la Productividad y al Rendimiento del Personal Académico de Asignatura.
(Nombre del Usuario 2)	**Jefe de División** Alfonso Ayala Rico Rosa Martha Barona Peña Silvia Berenice Villamil Rodríguez María del Rocío Huitrón Hernández Marlene Olga Ramírez Chavero **Coordinador de licenciatura** Alfonso Manuel Aguilar Guevara María Gloria Arévalo Guerrero Eva Elizabeth del Valle Córdova Graciela Enríquez Guadarrama Gabriel Guevara Gutiérrez Javier Isaac Osorio González Francisco Alberto Piña Salazar Pedro Eduardo Quezada García María Angélica Alicia Raya Sánchez Isaías Reyes Bojórquez Carlos Ruiz Díaz Carlos Ríos Murillo Alma Lucero Sosa Blancas Karen Gisel Velázquez Rojas Israel Vladimir Villa García Romeo Vite López **Coordinador de posgrado** Alfredo Corona Cabrera

	Scott Michel Martín Da Gama Darby Silvia Adriana Durand Bautista M. Cristina García García Francisco Gerardo Serrano Luis Alberto Gómez Alvarado María del Rosario Higuera Torres María Eugenia Miranda Jaimes María Amalia Belén Negrete Vargas José Padilla Hernández **Coordinador del SUAyED** Martha Patricia García Chavero Sara Guadalupe Espinosa de los Monteros Montes de Oca
Cargo:	Jefe de División, Coordinador académico de licenciatura, Coordinador académico de posgrado, Coordinador del SUAyED.
Funciones:	Consulta y visto bueno a los planes e informes de trabajo de las asignaturas que imparte el profesor. Comunicación con los profesores con aquellos que no han cumplido en tiempo con el registro del plan o informe de trabajo.
Obligaciones:	Mantener confidencialidad el nombre y el correo del profesor, usado para el cumplimiento de la entrega y visto bueno del plan e informe de trabajo académico.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIPIAD01**
(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades
Tipo de soporte:	El soporte es electrónico y vía telefónica.
Descripción:	Base de datos relacional
Características del lugar donde se resguardan los soportes:	Sitio dentro del Centro de Informática de la FCA ubicado en la planta baja, cuenta con aire acondicionado a 18° centígrados, el acceso es con puerta de marco laminado y con vidrio, cuenta con una cerradura sencilla, la llave y la copia es manejada por el Administrador de Servidores y el jefe del Centro de Informática.

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIPIAD01

(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades	
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPIAD01	
(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIPIAD01

[33] **Texto eliminado:** Apartado correspondiente a “Análisis de Riesgos, de Análisis de Brecha y del Plan de Trabajo” (páginas 126 a 127). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades		
Actividad	**Descripción**	**Duración**	**Cobertura**
[redacted]	[redacted]	[redacted]	[redacted]

MEDIDAS DE SEGURIDAD IMPLEMENTADAS
TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIPIAD01
(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica, no se reciben documentos o expedientes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No aplica, no se intercambian archivos electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de la información es por medio de una red pública y se considera posteriormente incluir red privada virtual (VPN).

RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El acceso al centro de datos y servidores es con llave y la chapa es sencilla, existe equipo de refrigeración que mantiene la temperatura a 18°, no existe un mecanismo para detección o supresión de incendios y cuenta con planta de luz y UPS.

Nombre	**Cargo**	**Funciones**	**Obligaciones**

[34] T**exto eliminado:** Apartado correspondiente a “Plan de Trabajo” (página 127). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Mtro. Balfred Santaella Hinojosa	Jefe del Centro de Informática	Planeación, organización y control de los sistemas de información de la Facultad.	Asegurar el funcionamiento de los sistemas y servicios de información.
Mtro. Germán Ignacio Cervantes González	Administrador de Servidores	Gestión, configuración, mantenimiento y soporte de los servidores y las bases de datos.	Revisar y mantener la correcta operación y disponibilidad de los servicios que dan soporte a los distintos sistemas de información.

BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**

   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   No se registran bitácoras en el sistema, se emplean los logs del servidor.

   b) Para soportes físicos: Número o clave del expediente utilizado, y
   No aplica.

   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
   No aplica.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
   Los logs del servidor como soporte electrónico.
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
   En el sistema operativo de red de manera semanal.
4. La manera en que asegura la integridad de las bitácoras, y
   Con respaldos semanales.
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
   Administrador de servidores.
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
   No hay herramientas de análisis.

REGISTRO DE INCIDENTES

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   Germán Ignacio Cervantes Gonzáles (Servidores) y/o Hugo Díaz García (Responsable del sistema)
   b) La metodología aplicada;
      i. Se genera un informe con los daños ocurridos y el equipo faltante en el centro de datos, a partir de que se pueda acceder a las instalaciones se genera una lista de los servidores dañados junto con los sistemas que se ven afectados y el inventario

del equipo.

ii. Del incidente se toman fotografías y se genera un acta por el o la abogad(a) de la facultad con el fin de denunciar los hechos ante el ministerio público, se informará al abogado general de UNAM y autoridades universitarias acerca de las afectaciones.

iii. Durante no más a 5 días naturales de ocurrido el incidente se hace pública la denuncia y es publicada en la página de la FCA informando a la comunidad de los hechos, así como del robo y/o daño de la información sustraída.

iv. En el caso de robo de datos personales se alertará a los titulares por medio de un correo masivo del evento para que tomen sus precauciones acerca del uso indebido de los datos personales.

v. En el caso de un ataque externo se le informa del incidente a la DGTIC para que se tomen medidas correctivas y precautorias.

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y

d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

Del incidente se revisa el servidor y los respaldos para conocer que se puede recuperar y que se debe reinstalar y restaurar.

2. Si el registro está en soporte físico o en soporte electrónico;
El registro esta en soporte electrónico.
3. Cómo asegura la integridad de dicho registro, y
Empleando un MD5 y revisando los últimos índices de las principales tablas.
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.
Mtro. Balfred Santaella Hinojosa (Jefe del Centro de Informática)

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado.

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales.

PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
No
b) ¿Es discrecional (matriz de control de acceso)?
No
c) ¿Está basado en roles (perfiles) o grupos?
Sí
d) ¿Está basado en reglas?

No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
No

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema

b) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema

c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí

c) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

5. Señalar si realiza respaldos

d) Completos_X_, diferenciales ___ o incrementales___;

e) De forma automática _____ o Manual __X___,

f) Periodicidad con que los realiza: ___semanal_____

6. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
Discos duros

7. Cómo y dónde archiva esos medios, y
Arreglos de discos

8. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
Administrador de servidores

PLAN DE CONTINGENCIA

No se cuenta con plan de contingencia, pero se planea desarrollarlo.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPIAD01	
(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades	
Recurso	**Descripción**	**Control**
NANGIOS	Monitorea los recursos y servicios de los servidores.	Lo lleva a cabo el administrador de servidores Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPIAD01	
(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades	
Medida de seguridad	**Procedimiento**	**Responsable**
No aplica.	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPIAD01	
(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPIAD01	
(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIPIAD01		
(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades		
Actividad	**Descripción**	**Duración**	**Cobertura**

La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIPIAD01		
(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir el enlace al aviso de privacidad	Se realiza de manera electrónica	Permanente	Usuarios del sistema

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIPIAD01		
(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso*	*Permanente*	*Usuarios del sistema*

	de privacidad vigente		

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIPIAD01		
(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	Se descargan e instalan de manera manual	Cada que se recibe notificación de un nuevo parche de seguridad	Mantener la integridad de los datos ante amenazas
Limpieza de logs	Se elimina información histórica de bitácoras	Mensual	Ayuda a liberar espacio de almacenamiento

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPIAD01	
(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades	
Proceso	**Descripción**	**Responsable**
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos*	*Administrador de servidores* *Mtro. Germán Ignacio Cervantes González*

	Se rotan los respaldos previos para dar entrada a los siguientes *Copiar un nuevo respaldo*	

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPIAD01	
(Nombre del sistema A12)	Sistema de información de proyecto e informe de actividades	
Proceso	**Descripción**	**Responsable**
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	Administrador de servidores *Mtro. Germán Ignacio Cervantes González*

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A13 SISTEMA DE INFORMACIÓN ADMINISTRATIVO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIA01**
Sistema (Nombre del A13):	Sistema de información administrativo
Datos personales contenidos en el sistema:	Datos de identificación. Proveedor: Nombre, apellido paterno, apellido materno, RFC.
Responsable:	
Nombre:	**Mtro. Balfred Santaella Hinojosa**

Cargo:	**Jefe del Centro de Informática**
Funciones:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1)	**Mtro. Hugo Díaz García**
Cargo:	Jefe de Sistemas
Funciones:	Soporte al área para el registro de datos para el registro de formas múltiples de ingresos extraordinarios y presupuesto. Manejo de la base de datos.
Obligaciones:	Almacenamiento e integridad de la información. Emplear los datos personales dentro el proceso definido y para los fines del sistema.
	Usuarios:
(Nombre del Usuario 1)	Administradores Tomas Aguilar Nápoles Héctor Mendoza Medina Fabiola Santillán Sosa
Cargo:	Jefe del Departamento de Presupuesto Asistente del Departamento de Presupuesto
Funciones:	Generar y consultar formas múltiples para el trámite de pago a proveedores.
Obligaciones:	Manejo de datos de proveedores para el registro de formas múltiples y manejo de ingresos o presupuesto.
(Nombre del Usuario 2)	Operador Ingresos Lic. Paola Yunuen Sandoval Tinoco
Cargo:	Asistente del Departamento de ingresos extraordinarios
Funciones:	• Generar y consultar formas múltiples para el trámite de pago a proveedores de ingresos extraordinarios.
Obligaciones:	• Manejo de datos de proveedores para el registro de formas múltiples y manejo de ingresos.
(Nombre del Usuario 3)	Operador Posgrado: Celia Marcial Jiménez María Zoila Rodríguez González
Cargo:	Responsable del Departamento de Contabilidad de la División de Estudios de Posgrado Responsable del Área de Presupuesto de la División de Estudios de Posgrado
Funciones:	Generar y consultar formas múltiples para el trámite de pago a proveedores de ingresos extraordinarios de posgrado.
Obligaciones:	Manejo de datos de proveedores para el registro de formas múltiples y manejo de ingresos de posgrado.
(Nombre del Usuario 4)	Operador DEC Joel Suárez Estrada
Cargo:	Coordinación administrativa
Funciones:	Generar y consultar formas múltiples para el trámite de pago a proveedores de ingresos extraordinarios de la División de Educación Continua.
Obligaciones:	Manejo de datos de proveedores para el registro de formas

	múltiples y manejo de ingresos de la División de Educación Continua.
(Nombre del Usuario 5)	Consulta Karla Fajardo Morales
Cargo:	Jefa del Departamento de Ingresos Extraordinarios
Funciones:	Consultar formas múltiples para el trámite de pago a proveedores de ingresos extraordinarios.
Obligaciones:	Consulta de datos de proveedores para el trámite de formas múltiples y manejo de ingresos extraordinarios.
(Nombre del Usuario 6)	Consulta Jann Miguel Montes Barrios Lucero Vázquez Díaz
Cargo:	Contabilidad
Funciones:	Consultar formas múltiples para el trámite de pago a proveedores de ingresos extraordinarios o presupuesto.
Obligaciones:	Consulta de datos de proveedores para el trámite de formas múltiples y manejo de ingresos extraordinarios o presupuesto.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIA01**
(Nombre del sistema A12)	Sistema de información administrativo
Tipo de soporte:	El soporte es electrónico y vía telefónica.
Descripción:	Base de datos relacional
Características del lugar donde se resguardan los soportes:	Sitio dentro del Centro de Informática de la FCA ubicado en la planta baja, cuenta con aire acondicionado a 18° centígrados, el acceso es con puerta de marco laminado y con vidrio, cuenta con una cerradura sencilla, la llave y la copia es manejada por el Administrador de Servidores y el jefe del Centro de Informática.

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIA01	
(Nombre del sistema A13)	Sistema de información administrativo	
Riesgo	**Impacto**	**Mitigación**

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

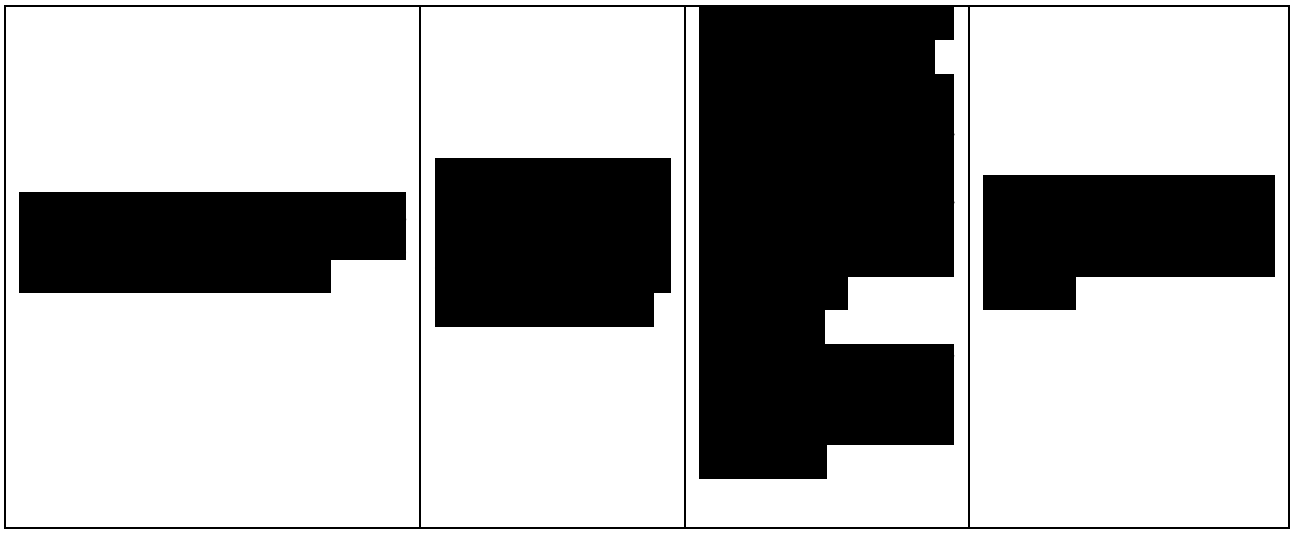
ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIA01	
(Nombre del sistema A13)	Sistema de información administrativo	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIA01		
(Nombre del sistema A13)	Sistema de información administrativo		
Actividad	**Descripción**	**Duración**	**Cobertura**

[35] T**exto eliminado:** Apartado correspondiente a “Análisis de Riesgos, de Análisis de Brecha y del Plan de Trabajo” (páginas 138 a 139). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.



MEDIDAS DE SEGURIDAD IMPLEMENTADAS

TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIA01
(Nombre del sistema A13)	Sistema de información administrativo
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica, no se reciben documentos o expedientes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No aplica, no se intercambian archivos electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de la información es por medio de una red pública y se considera posteriormente incluir red privada virtual (VPN).

RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El acceso al centro de datos y servidores es con llave y la chapa es sencilla, existe equipo de refrigeración que mantiene la temperatura a 18°, no existe un mecanismo para detección o supresión de incendios y cuenta con planta de luz y UPS.

Nombre	Cargo	Funciones	Obligaciones
Mtro. Balfred Santaella Hinojosa	Jefe del Centro de Informática	Planeación, organización y control de los sistemas de	Asegurar el funcionamiento de los sistemas y servicios de información.

[36] T**exto eliminado:** Apartado correspondiente a “Plan de Trabajo” (página 139). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

		información de la Facultad.	
Mtro. Germán Ignacio Cervantes González	Administrador de Servidores	Gestión, configuración, mantenimiento y soporte de los servidores y las bases de datos.	Revisar y mantener la correcta operación y disponibilidad de los servicios que dan soporte a los distintos sistemas de información.

BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**

   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   No se registran bitácoras en el sistema, se emplean los logs del servidor.

   b) Para soportes físicos: Número o clave del expediente utilizado, y
   No aplica.

   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
   No aplica.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
   Los logs del servidor como soporte electrónico.
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
   En el sistema operativo de red de manera semanal.
4. La manera en que asegura la integridad de las bitácoras, y
   Con respaldos semanales.
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
   Administrador de servidores.
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
   No hay herramientas de análisis.

REGISTRO DE INCIDENTES

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   Germán Ignacio Cervantes Gonzáles (Servidores) y/o Hugo Díaz García (Responsable del sistema)
   b) La metodología aplicada;
   - **i.** Se genera un informe con los daños ocurridos y el equipo faltante en el centro de datos, a partir de que se pueda acceder a las instalaciones se genera una lista de los servidores dañados junto con los sistemas que se ven afectados y el inventario del equipo.
   - **ii.** Del incidente se toman fotografías y se genera un acta por el o la abogad(a) de la

facultad con el fin de denunciar los hechos ante el ministerio público, se informará al abogado general de UNAM y autoridades universitarias acerca de las afectaciones.

iii. Durante no más a 5 días naturales de ocurrido el incidente se hace pública la denuncia y es publicada en la página de la FCA informando a la comunidad de los hechos, así como del robo y/o daño de la información sustraída.

iv. En el caso de robo de datos personales se alertará a los titulares por medio de un correo masivo del evento para que tomen sus precauciones acerca del uso indebido de los datos personales.

v. En el caso de un ataque externo se le informa del incidente a la DGTIC para que se tomen medidas correctivas y precautorias.

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y

d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

Del incidente se revisa el servidor y los respaldos para conocer que se puede recuperar y que se debe reinstalar y restaurar.

2. Si el registro está en soporte físico o en soporte electrónico;
El registro esta en soporte electrónico.
3. Cómo asegura la integridad de dicho registro, y
Empleando un MD5 y revisando los últimos índices de las principales tablas.
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.
Mtro. Balfred Santaella Hinojosa (Jefe del Centro de Informática)

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado.

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales.

PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
No
b) ¿Es discrecional (matriz de control de acceso)?
No
c) ¿Está basado en roles (perfiles) o grupos?
Sí
d) ¿Está basado en reglas?
No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
No

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema

b) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema

c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí

c) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_X_, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual __X___,
   c) Periodicidad con que los realiza: ___semanal____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;
   Discos duros
3. Cómo y dónde archiva esos medios, y
   Arreglos de discos
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Administrador de servidores

PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   No se cuenta con plan de contingencia, pero se planea desarrollarlo.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   No aplica.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío)
   b) Si el sitio es propio o subcontratado con un tercero;
   c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
   d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

No aplica.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAD01	
(Nombre del sistema A13)	Sistema de información administrativo	
Recurso	**Descripción**	**Control**
NANGIOS	Monitorea los recursos y servicios de los servidores.	Lo lleva a cabo el administrador de servidores Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIA01

(Nombre del sistema A13)	Sistema de información administrativo	
Medida de seguridad	**Procedimiento**	**Responsable**
No aplica.	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIA01	
(Nombre del sistema A13)	Sistema de información administrativo	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIA01	
(Nombre del sistema A13)	Sistema de información administrativo	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIA01		
(Nombre del sistema A13)	Sistema de información administrativo		
Actividad	**Descripción**	**Duración**	**Cobertura**
La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIA01		
(Nombre del sistema A13)	Sistema de información administrativo		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir el enlace al aviso de privacidad	Se realiza de manera electrónica	Permanente	Usuarios del sistema

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIA01		
(Nombre del sistema A13)	Sistema de información administrativo		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso de privacidad vigente*	*Permanente*	*Usuarios del sistema*

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIA01		
(Nombre del sistema A13)	Sistema de información administrativo		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	Se descargan e instalan de manera manual	Cada que se recibe notificación de un nuevo parche de seguridad	Mantener la integridad de los datos ante amenazas
Limpieza de logs	Se elimina información histórica de bitácoras	Mensual	Ayuda a liberar espacio de almacenamiento

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIA01	
(Nombre del sistema A13)	Sistema de información administrativo	
Proceso	**Descripción**	**Responsable**
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes* *Copiar un nuevo respaldo*	*Administrador de servidores* *Mtro. Germán Ignacio Cervantes González*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIA01	
(Nombre del sistema A13)	Sistema de información administrativo	
Proceso	**Descripción**	**Responsable**
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	Administrador de servidores *Mtro. Germán Ignacio Cervantes González*

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A14 SISTEMA DE INFORMACIÓN AUDITORIOS Y SERVICIOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIAS01**
Sistema (Nombre del A14):	Sistema de información auditorios y servicios
Datos personales contenidos en el sistema:	Datos de identificación. Personal de tiempo completo: Nombre, apellido paterno, apellido materno, para reservar auditorios con los servicios a emplear.
Responsable:	
Nombre:	**Mtro. Balfred Santaella Hinojosa**
Cargo:	**Jefe del Centro de Informática**
Funciones:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1)	**Mtro. Hugo Díaz García**
Cargo:	Jefe de Sistemas
Funciones:	Soporte al área para la reservación de auditorios a través del personal registrado para el uso de los mismos. Manejo de la base de datos.
Obligaciones:	Almacenamiento e integridad de la información. Emplear los datos personales dentro el proceso definido y para los fines del sistema.
	Usuarios:
(Nombre del Usuario 1)	José Ricardo Méndez Cruz
Cargo:	Secretario de Divulgación y Fomento Editorial
Funciones:	Alta de personal de tiempo completo para que puedan realizar la reservación de un recinto.
Obligaciones:	Consulta del nombre completo del personal de tiempo completo para la alta de cuentas.
(Nombre del Usuario 2)	Múltiples usuarios
Cargo:	Autorizador (Varios)
Funciones:	Autorizar al personal de tiempo completo la solicitud de un espacio para un recinto.
Obligaciones:	Consulta del solicitante para la reservación del espacio.
(Nombre del Usuario 3)	Múltiples usuarios
Cargo:	Operador (Varios)
Funciones:	Solicita un espacio para un recinto.
Obligaciones:	Ninguna en cuanto a datos personales.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIAS01**
(Nombre del sistema A14)	Sistema de información de auditorios y servicios
Tipo de soporte:	El soporte es electrónico y vía telefónica.
Descripción:	Base de datos relacional
Características del lugar donde se resguardan los soportes:	Sitio dentro del Centro de Informática de la FCA ubicado en la planta baja, cuenta con aire acondicionado a 18° centígrados, el acceso es con puerta de marco laminado y con vidrio, cuenta con una cerradura sencilla, la llave y la copia es manejada por el Administrador de Servidores y el jefe del Centro de Informática.

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAS01	
(Nombre del sistema A14)	Sistema de información de auditorios y servicios	
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)

[37] **Texto eliminado:** Apartado correspondiente a “Análisis de Riesgos y de Análisis de Brecha” (páginas 149 a 150). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Identificador único	FCASIAS01	
(Nombre del sistema A14)	Sistema de información auditorios y servicios	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIAS01		
(Nombre del sistema A14)	Sistema de información auditorios y servicios		
Actividad	**Descripción**	**Duración**	**Cobertura**
[redacted]	[redacted]	[redacted]	[redacted]

MEDIDAS DE SEGURIDAD IMPLEMENTADAS
TRANSFERENCIAS DE DATOS PERSONALES

[38] T**exto eliminado:** Apartado correspondiente a “Análisis de Brecha y del Plan de Trabajo” (página 150). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIAS01
(Nombre del sistema A14)	Sistema de información auditorios y servicios
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica, no se reciben documentos o expedientes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No aplica, no se intercambian archivos electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de la información es por medio de una red pública y se considera posteriormente incluir red privada virtual (VPN).

RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El acceso al centro de datos y servidores es con llave y la chapa es sencilla, existe equipo de refrigeración que mantiene la temperatura a 18°, no existe un mecanismo para detección o supresión de incendios y cuenta con planta de luz y UPS.

Nombre	Cargo	Funciones	Obligaciones
Mtro. Balfred Santaella Hinojosa	Jefe del Centro de Informática	Planeación, organización y control de los sistemas de información de la Facultad.	Asegurar el funcionamiento de los sistemas y servicios de información.
Mtro. Germán Ignacio Cervantes González	Administrador de Servidores	Gestión, configuración, mantenimiento y soporte de los servidores y las bases de datos.	Revisar y mantener la correcta operación y disponibilidad de los servicios que dan soporte a los distintos sistemas de información.

BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Los datos que se registran en las bitácoras:

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
No se registran bitácoras en el sistema, se emplean los logs del servidor.

b) Para soportes físicos: Número o clave del expediente utilizado, y
No aplica.

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
No aplica.

1. Si las bitácoras están en soporte físico o en soporte electrónico;
Los logs del servidor como soporte electrónico.
2. Lugar dónde almacena las bitácoras y por cuánto tiempo;
En el sistema operativo de red de manera semanal.
3. La manera en que asegura la integridad de las bitácoras, y
Con respaldos semanales.
4. Respecto del análisis de las bitácoras:
a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
Administrador de servidores.
b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
No hay herramientas de análisis.

REGISTRO DE INCIDENTES

1. Los datos que registra:
a) La persona que resolvió el incidente;
Germán Ignacio Cervantes Gonzáles (Servidores) y/o Hugo Díaz García (Responsable del sistema)
b) La metodología aplicada;
i. Se genera un informe con los daños ocurridos y el equipo faltante en el centro de datos, a partir de que se pueda acceder a las instalaciones se genera una lista de los servidores dañados junto con los sistemas que se ven afectados y el inventario del equipo.
ii. Del incidente se toman fotografías y se genera un acta por el o la abogad(a) de la facultad con el fin de denunciar los hechos ante el ministerio público, se informará al abogado general de UNAM y autoridades universitarias acerca de las afectaciones.
iii. Durante no más a 5 días naturales de ocurrido el incidente se hace pública la denuncia y es publicada en la página de la FCA informando a la comunidad de los hechos, así como del robo y/o daño de la información sustraída.
iv. En el caso de robo de datos personales se alertará a los titulares por medio de un correo masivo del evento para que tomen sus precauciones acerca del uso indebido de los datos personales.
v. En el caso de un ataque externo se le informa del incidente a la DGTIC para que se tomen medidas correctivas y precautorias.
c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.
Del incidente se revisa el servidor y los respaldos para conocer que se puede recuperar y que se debe reinstalar y restaurar.
2. Si el registro está en soporte físico o en soporte electrónico;
El registro esta en soporte electrónico.
3. Cómo asegura la integridad de dicho registro, y
Empleando un MD5 y revisando los últimos índices de las principales tablas.
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.
Mtro. Balfred Santaella Hinojosa (Jefe del Centro de Informática)

ACCESO A LAS INSTALACIONE

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado.

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales.

PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
No
b) ¿Es discrecional (matriz de control de acceso)?
No
c) ¿Está basado en roles (perfiles) o grupos?
Sí
d) ¿Está basado en reglas?
No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
No
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema
b) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema
c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?

No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí

c) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_X_, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual __X___,
   c) Periodicidad con que los realiza: ___semanal____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;
   Discos duros
3. Cómo y dónde archiva esos medios, y
   Arreglos de discos
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Administrador de servidores

PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   No se cuenta con plan de contingencia, pero se planea desarrollarlo.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   No aplica.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);
   b) Si el sitio es propio o subcontratado con un tercero;
   c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
   d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.
   No aplica.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)

Identificador único	FCASIAS01	
(Nombre del sistema A14)	Sistema de información de auditorios y servicios	
Recurso	**Descripción**	**Control**
NANGIOS	Monitorea los recursos y servicios de los servidores.	Lo lleva a cabo el administrador de servidores Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAS01	
(Nombre del sistema A14)	Sistema de información de auditorios y servicios	
Medida de seguridad	**Procedimiento**	**Responsable**
No aplica.	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAS01	
(Nombre del sistema A14)	Sistema de información de auditorios y servicios	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAS01	
(Nombre del sistema A14)	Sistema de información de auditorios y servicios	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*No aplica*

Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIAS01		
(Nombre del sistema A14)	Sistema de información auditorios y servicios		
Actividad	**Descripción**	**Duración**	**Cobertura**
La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIAS01

(Nombre del sistema A14)	Sistema de información de auditorios y servicios		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir el enlace al aviso de privacidad	Se realiza de manera electrónica	Permanente	Usuarios del sistema

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIAS01		
(Nombre del sistema A14)	Sistema de información de auditorios y servicios		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso de privacidad vigente*	*Permanente*	*Usuarios del sistema*

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIAS01		
(Nombre del sistema A14)	Sistema de información de auditorios y servicios		
Actividad	**Descripción**	**Duración**	**Cobertura**

Instalación de parches de seguridad	Se descargan e instalan de manera manual	Cada que se recibe notificación de un nuevo parche de seguridad	Mantener la integridad de los datos ante amenazas
Limpieza de logs	Se elimina información histórica de bitácoras	Mensual	Ayuda a liberar espacio de almacenamiento

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAS01	
(Nombre del sistema A14)	Sistema de información de auditorios y servicios	
Proceso	**Descripción**	**Responsable**
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes* *Copiar un nuevo respaldo*	*Administrador de servidores* *Mtro. Germán Ignacio Cervantes González*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIAS01
(Nombre del sistema A14)	Sistema de información auditorios y servicios

Proceso	Descripción	Responsable
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	Administrador de servidores *Mtro. Germán Ignacio Cervantes González*

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A15 SISTEMA DE INFORMACIÓN DEL DIRECTORIO ELECTRÓNICO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIDE01**
Sistema (Nombre del A15):	Sistema de información del directorio electrónico
Datos personales contenidos en el sistema:	Datos de identificación. Personal de tiempo completo: Nombre, apellido paterno, apellido materno, teléfono oficina y correo institucional para informes y contacto con la comunidad universitaria y público en general.
Responsable:	
Nombre:	**Mtro. Balfred Santaella Hinojosa**
Cargo:	**Jefe del Centro de Informática**
Funciones:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1)	**Mtro. Hugo Díaz García**
Cargo:	Jefe de Sistemas
Funciones:	Soporte al área para la publicación del personal de tiempo completo. Manejo de la base de datos.
Obligaciones:	Almacenamiento e integridad de la información. Emplear los datos personales del personal de tiempo completo dentro el proceso definido y para los fines del sistema.

	Usuarios:
(Nombre del Usuario 1)	José Ricardo Méndez Cruz
Cargo:	Secretario de Divulgación y Fomento Editorial
Funciones:	Gestión del personal de tiempo completo para cambios de personal y de datos de contacto laborales.
Obligaciones:	Mantener actualizado el directorio acerca del personal de tiempo completo para la presentación en el directorio de la facultad.
(Nombre del Usuario 2)	Operador Iván Ventura González López
Cargo:	Editor y corrector de Estilo
Funciones:	Actualizar los datos personales de contacto para su comunicación.
Obligaciones:	Mantener actualizado el directorio acerca del personal de tiempo completo para la presentación en el directorio de la facultad.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIDES01**
(Nombre del sistema A15)	Sistema de información del directorio electrónico
Tipo de soporte:	El soporte es electrónico y vía telefónica.
Descripción:	Base de datos relacional
Características del lugar donde se resguardan los soportes:	Sitio dentro del Centro de Informática de la FCA ubicado en la planta baja, cuenta con aire acondicionado a 18° centígrados, el acceso es con puerta de marco laminado y con vidrio, cuenta con una cerradura sencilla, la llave y la copia es manejada por el Administrador de Servidores y el jefe del Centro de Informática.

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIDE01	
(Nombre del sistema A15)	Sistema de información del directorio de electrónico	
Riesgo	**Impacto**	**Mitigación**

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

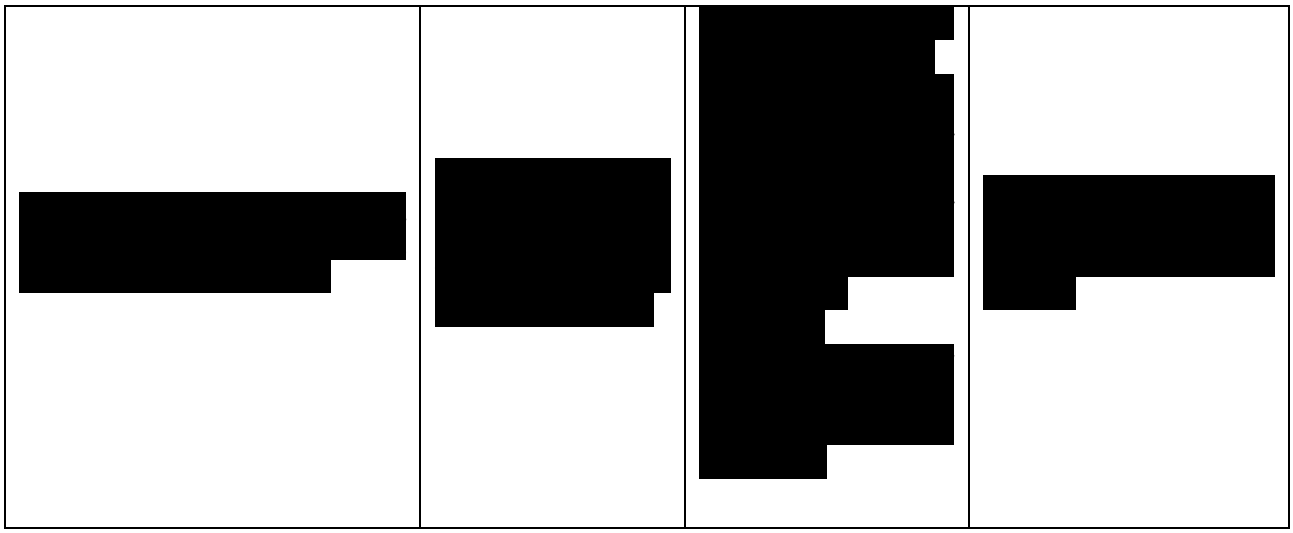
ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIDE01	
(Nombre del sistema A15)	Sistema de información del directorio electrónico	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIDE01		
(Nombre del sistema A15)	Sistema de información del directorio electrónico		
Actividad	**Descripción**	**Duración**	**Cobertura**

[39] **Texto eliminado:** Apartado correspondiente a “Análisis de Riesgos, de Análisis de Brecha y del Plan de Trabajo” (páginas 161 a 162). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.



MEDIDAS DE SEGURIDAD IMPLEMENTADAS

TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIDE01
(Nombre del sistema A15)	Sistema de información del directorio electrónico
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica, no se reciben documentos o expedientes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No aplica, no se intercambian archivos electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de la información es por medio de una red pública y se considera posteriormente incluir red privada virtual (VPN).

RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El acceso al centro de datos y servidores es con llave y la chapa es sencilla, existe equipo de refrigeración que mantiene la temperatura a 18°, no existe un mecanismo para detección o supresión de incendios y cuenta con planta de luz y UPS.

Nombre	Cargo	Funciones	Obligaciones
Mtro. Balfred Santaella Hinojosa	Jefe del Centro de Informática	Planeación, organización y control de los sistemas de	Asegurar el funcionamiento de los sistemas y servicios de información.

[40] T**exto eliminado:** Apartado correspondiente a “Plan de Trabajo” (página 162). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

		información de la Facultad.	
Mtro. Germán Ignacio Cervantes González	Administrador de Servidores	Gestión, configuración, mantenimiento y soporte de los servidores y las bases de datos.	Revisar y mantener la correcta operación y disponibilidad de los servicios que dan soporte a los distintos sistemas de información.

BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**
   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   No se registran bitácoras en el sistema, se emplean los logs del servidor.

   b) Para soportes físicos: Número o clave del expediente utilizado, y
   No aplica.

   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
   No aplica.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
   Los logs del servidor como soporte electrónico.
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
   En el sistema operativo de red de manera semanal.
4. La manera en que asegura la integridad de las bitácoras, y
   Con respaldos semanales.
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
   Administrador de servidores.
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
   No hay herramientas de análisis.

REGISTRO DE INCIDENTES

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   Germán Ignacio Cervantes Gonzáles (Servidores) y/o Hugo Díaz García (Responsable del sistema)
   b) La metodología aplicada;
   - **i.** Se genera un informe con los daños ocurridos y el equipo faltante en el centro de datos, a partir de que se pueda acceder a las instalaciones se genera una lista de los servidores dañados junto con los sistemas que se ven afectados y el inventario del equipo.
   - **ii.** Del incidente se toman fotografías y se genera un acta por el o la abogad(a) de la facultad con el fin de denunciar los hechos ante el ministerio público, se informará al abogado general de UNAM y autoridades universitarias acerca de las afectaciones.

iii. Durante no más a 5 días naturales de ocurrido el incidente se hace pública la denuncia y es publicada en la página de la FCA informando a la comunidad de los hechos, así como del robo y/o daño de la información sustraída.

iv. En el caso de robo de datos personales se alertará a los titulares por medio de un correo masivo del evento para que tomen sus precauciones acerca del uso indebido de los datos personales.

v. En el caso de un ataque externo se le informa del incidente a la DGTIC para que se tomen medidas correctivas y precautorias.

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y

d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

Del incidente se revisa el servidor y los respaldos para conocer que se puede recuperar y que se debe reinstalar y restaurar.

2. Si el registro está en soporte físico o en soporte electrónico;
El registro esta en soporte electrónico.
3. Cómo asegura la integridad de dicho registro, y
Empleando un MD5 y revisando los últimos índices de las principales tablas.
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.
Mtro. Balfred Santaella Hinojosa (Jefe del Centro de Informática)

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado.

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales.

PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
No
b) ¿Es discrecional (matriz de control de acceso)?
No
c) ¿Está basado en roles (perfiles) o grupos?
Sí
d) ¿Está basado en reglas?
No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?

Sí

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
No

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema

b) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema

c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí

c) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_X_, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual __X___,
   c) Periodicidad con que los realiza: ___semanal____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Discos duros
3. Cómo y dónde archiva esos medios, y
   Arreglos de discos
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Administrador de servidores

PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   No se cuenta con plan de contingencia, pero se planea desarrollarlo.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   No aplica.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);
   b) Si el sitio es propio o subcontratado con un tercero;
   c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
   d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

No aplica.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIAS01	
(Nombre del sistema A15)	Sistema de información del directorio electrónico	
Recurso	**Descripción**	**Control**
NANGIOS	Monitorea los recursos y servicios de los servidores.	Lo lleva a cabo el administrador de servidores Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIDES01

(Nombre del sistema A15)	Sistema de información del directorio electrónico	
Medida de seguridad	**Procedimiento**	**Responsable**
No aplica.	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIDES01	
(Nombre del sistema A15)	Sistema de información del directorio electrónico	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIDES01	
(Nombre del sistema A15)	Sistema de información del directorio electrónico	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN
Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIDE01		
(Nombre del sistema A15)	Sistema de información del directorio electrónico		
Actividad	**Descripción**	**Duración**	**Cobertura**
La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIDES01		
(Nombre del sistema A15)	Sistema de información del directorio electrónico		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir el enlace al aviso de privacidad	Se realiza de manera electrónica	Permanente	Usuarios del sistema

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIDE01

(Nombre del sistema A15)	Sistema de información del directorio electrónico		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso de privacidad vigente*	*Permanente*	*Usuarios del sistema*

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIDE01		
(Nombre del sistema A15)	Sistema de información del directorio electrónico		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	Se descargan e instalan de manera manual	Cada que se recibe notificación de un nuevo parche de seguridad	Mantener la integridad de los datos ante amenazas
Limpieza de logs	Se elimina información histórica de bitácoras	Mensual	Ayuda a liberar espacio de almacenamiento

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIDE01

(Nombre del sistema A15)	Sistema de información del directorio electrónico	
Proceso	**Descripción**	**Responsable**
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes* *Copiar un nuevo respaldo*	*Administrador de servidores* *Mtro. Germán Ignacio Cervantes González*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIDE01	
(Nombre del sistema A15)	Sistema de información del directorio electrónico	
Proceso	**Descripción**	**Responsable**
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	Administrador de servidores *Mtro. Germán Ignacio Cervantes González*

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A16 SISTEMA DE INFORMACIÓN DEL DIRECTORIO ELECTRÓNICO DE ANFECA (ASOCIACIÓN NACIONAL DE FACULTADES Y ESCUELAS EN CONTADURÍA Y ADMINISTRACIÓN)

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)

Identificador único	**FCASIDEANFECA01**
Sistema (Nombre del A16):	Sistema de información del directorio electrónico de ANFECA (Asociación Nacional de Facultades y Escuelas en Contaduría y Administración)
Datos personales contenidos en el sistema:	Datos de identificación. Nombre, apellido paterno, apellido materno, CURP, teléfono oficina y correo institucional para los miembros afiliados a ANFECA.
Responsable:	
Nombre:	**Mtro. Balfred Santaella Hinojosa**
Cargo:	**Jefe del Centro de Informática**
Funciones:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1)	**Mtro. Hugo Díaz García**
Cargo:	Jefe de Sistemas
Funciones:	Soporte al área para la afiliación de personal que representa una institución afiliada a ANFECA. Manejo de la base de datos.
Obligaciones:	Almacenamiento e integridad de la información. Emplear los datos personales de los representantes institucionales dentro el proceso definido y para los fines del sistema.
	Usuarios:
(Nombre del Usuario 1)	Administrador Mtro. Carlos Lobo Sánchez
Cargo:	Director Ejecutivo de ANFECA
Funciones:	Gestión del personal representante de ANFECA para la actualización de afiliados y sus datos de contacto.
Obligaciones:	Mantener actualizado los directorios (Consejo Nacional Directivo, Consejos Regionales, Instituciones y Coordinaciones) de los miembros afiliados para la presentación en el directorio de la ANFECA.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIDEANFECA01**

(Nombre del sistema A16)	Sistema de información del directorio electrónico de la ANFECA
Tipo de soporte:	El soporte es electrónico y vía telefónica.
Descripción:	Base de datos relacional
Características del lugar donde se resguardan los soportes:	Sitio dentro del Centro de Informática de la FCA ubicado en la planta baja, cuenta con aire acondicionado a 18° centígrados, el acceso es con puerta de marco laminado y con vidrio, cuenta con una cerradura sencilla, la llave y la copia es manejada por el Administrador de Servidores y el jefe del Centro de Informática.

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIDEANFECA01	
(Nombre del sistema A16)	Sistema de información del directorio de electrónico de la Asociación Nacional de Escuelas y Facultades en Contaduría	
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIDEANFECA01

[41] T**exto eliminado:** Apartado correspondiente a “Análisis de Riesgos y de Análisis de Brecha” (páginas 172 a 173). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

(Nombre del sistema A16)	Sistema de información del directorio electrónico para la Asociación Nacional de Escuelas y Facultades en Contaduría y Administración.	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIDEANFECA01		
(Nombre del sistema A16)	Sistema de información del directorio electrónico para la ANFECA.		
Actividad	**Descripción**	**Duración**	**Cobertura**
[redacted]	[redacted]	[redacted]	[redacted]

[42] **Texto eliminado:** Apartado correspondiente a "Análisis de Brecha y del Plan de Trabajo" (página 173). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

MEDIDAS DE SEGURIDAD IMPLEMENTADAS

TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIDEANFECA01
(Nombre del sistema A16)	Sistema de información del directorio electrónico para la ANFECA
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica, no se reciben documentos o expedientes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No aplica, no se intercambian archivos electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de la información es por medio de una red pública y se considera posteriormente incluir red privada virtual (VPN).

RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El acceso al centro de datos y servidores es con llave y la chapa es sencilla, existe equipo de refrigeración que mantiene la temperatura a 18°, no existe un mecanismo para detección o supresión de incendios y cuenta con planta de luz y UPS.

Nombre	Cargo	Funciones	Obligaciones
Mtro. Balfred Santaella Hinojosa	Jefe del Centro de Informática	Planeación, organización y control de los sistemas de información de la Facultad.	Asegurar el funcionamiento de los sistemas y servicios de información.
Mtro. Germán Ignacio Cervantes González	Administrador de Servidores	Gestión, configuración, mantenimiento y soporte de los servidores y las bases de datos.	Revisar y mantener la correcta operación y disponibilidad de los servicios que dan soporte a los distintos sistemas de información.

BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**
   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   No se registran bitácoras en el sistema, se emplean los logs del servidor.

   b) Para soportes físicos: Número o clave del expediente utilizado, y

No aplica.

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
No aplica.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
Los logs del servidor como soporte electrónico.
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
En el sistema operativo de red de manera semanal.
4. La manera en que asegura la integridad de las bitácoras, y
Con respaldos semanales.
5. Respecto del análisis de las bitácoras:
a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
Administrador de servidores.
b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
No hay herramientas de análisis.

REGISTRO DE INCIDENTES

1. Los datos que registra:
a) La persona que resolvió el incidente;
Germán Ignacio Cervantes Gonzáles (Servidores) y/o Hugo Díaz García (Responsable del sistema)
b) La metodología aplicada;
i. Se genera un informe con los daños ocurridos y el equipo faltante en el centro de datos, a partir de que se pueda acceder a las instalaciones se genera una lista de los servidores dañados junto con los sistemas que se ven afectados y el inventario del equipo.
ii. Del incidente se toman fotografías y se genera un acta por el o la abogad(a) de la facultad con el fin de denunciar los hechos ante el ministerio público, se informará al abogado general de UNAM y autoridades universitarias acerca de las afectaciones.
iii. Durante no más a 5 días naturales de ocurrido el incidente se hace pública la denuncia y es publicada en la página de la FCA informando a la comunidad de los hechos, así como del robo y/o daño de la información sustraída.
iv. En el caso de robo de datos personales se alertará a los titulares por medio de un correo masivo del evento para que tomen sus precauciones acerca del uso indebido de los datos personales.
v. En el caso de un ataque externo se le informa del incidente a la DGTIC para que se tomen medidas correctivas y precautorias.
c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.
Del incidente se revisa el servidor y los respaldos para conocer que se puede recuperar y que se debe reinstalar y restaurar.
2. Si el registro está en soporte físico o en soporte electrónico;
El registro esta en soporte electrónico.
3. Cómo asegura la integridad de dicho registro, y
Empleando un MD5 y revisando los últimos índices de las principales tablas.
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.
Mtro. Balfred Santaella Hinojosa (Jefe del Centro de Informática)

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado.

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

Para las personas que acceden a dichos espacios interiores:

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales.

PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
No
b) ¿Es discrecional (matriz de control de acceso)?
No
c) ¿Está basado en roles (perfiles) o grupos?
Sí
d) ¿Está basado en reglas?
No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
No
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema
b) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema

c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí

c) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_X_, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual __X___,
   c) Periodicidad con que los realiza: ___semanal____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Discos duros
3. Cómo y dónde archiva esos medios, y
   Arreglos de discos
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Administrador de servidores

PLAN DE CONTINGENCIA

No se cuenta con plan de contingencia, pero se planea desarrollarlo.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIDEANFECA01
(Nombre del sistema A16)	Sistema de información del directorio electrónico de la ANFECA

Recurso	Descripción	Control
NANGIOS	Monitorea los recursos y servicios de los servidores.	Lo lleva a cabo el administrador de servidores Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIDEANFECA01	
(Nombre del sistema A16)	Sistema de información del directorio electrónico de la ANFECA	
Medida de seguridad	**Procedimiento**	**Responsable**
No aplica.	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIDEANFECA01	
(Nombre del sistema A16)	Sistema de información del directorio electrónico de la ANFECA	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIDEANFECA01	
(Nombre del sistema A16)	Sistema de información del directorio electrónico de la ANFECA	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN
Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIDEANFECA01		
(Nombre del sistema A16)	Sistema de información del directorio electrónico de ANFECA		
Actividad	**Descripción**	**Duración**	**Cobertura**
La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIDEANFECA01		
(Nombre del sistema A19)	Sistema de información del directorio electrónico de la ANFECA		
Actividad	**Descripción**	**Duración**	**Cobertura**

Incluir el enlace al aviso de privacidad	Se realiza de manera electrónica	Permanente	Usuarios del sistema

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIDEANFECA01		
(Nombre del sistema A16)	Sistema de información del directorio electrónico de la ANFECA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso de privacidad vigente*	*Permanente*	*Usuarios del sistema*

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIDEANFECA01		
(Nombre del sistema A16)	Sistema de información del directorio electrónico de la ANFECA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	Se descargan e instalan de manera manual	Cada que se recibe notificación de un nuevo parche de seguridad	Mantener la integridad de los datos ante amenazas

Limpieza de logs	Se elimina información histórica de bitácoras	Mensual	Ayuda a liberar espacio de almacenamiento

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIDEANFECA01	
(Nombre del sistema A16)	Sistema de información del directorio electrónico de la ANFECA	
Proceso	**Descripción**	**Responsable**
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes* *Copiar un nuevo respaldo*	*Administrador de servidores* *Mtro. Germán Ignacio Cervantes González*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIDEANFECA01	
(Nombre del sistema A16)	Sistema de información del directorio electrónico de ANFECA	
Proceso	**Descripción**	**Responsable**
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	Administrador de servidores

		Mtro. Germán Ignacio Cervantes González

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

A17 SISTEMA DE INFORMACIÓN DEL PROCESO DE CERTIFICACIÓN ACADÉMICA DE LA ANFECA (ASOCIACIÓN NACIONAL DE FACULTADES Y ESCUELAS EN CONTADURÍA Y ADMINISTRACIÓN)

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIPCA01**
Sistema (Nombre del A17):	Sistema de información del proceso de certificación académica de la ANFECA (Asociación Nacional de Facultades y Escuelas en Contaduría y Administración)
Datos personales contenidos en el sistema:	Datos de identificación. Nombre, apellido paterno, apellido materno, CURP, calle, número, colonia, delegación, estado, teléfono fijo y móvil, y correo electrónico.
Responsable:	
Nombre:	**Mtro. Balfred Santaella Hinojosa**
Cargo:	**Jefe del Centro de Informática**
Funciones:	Planeación, organización y control de los sistemas de información de la Facultad
Obligaciones:	Asegurar el funcionamiento de los sistemas y servicios de información
	Encargados:
(Nombre del Encargado 1)	**Mtro. Hugo Díaz García**
Cargo:	Jefe de Sistemas
Funciones:	Soporte al área para el registro de académicos que representan solicitud para la certificación académica de la ANFECA. Manejo de la base de datos.
Obligaciones:	Almacenamiento e integridad de la información. Emplear los datos personales dentro el proceso definido y para los fines del sistema.
	Usuarios:
(Nombre del Usuario 1)	Administrador Mtro. Víctor Godínez Paredes

Cargo:	Secretario Ejecutivo de ANFECA
Funciones:	Consultar las solicitudes de los académicos registrados al proceso de certificación de ANFECA.
Obligaciones:	Mantener confidencial la información de los académicos y emplearla para el proceso de certificación que otorga la ANFECA.
(Nombre del Usuario 2)	Coordinador (Múltiples usuarios)
Cargo:	Coordinador Regional de ANFECA
Funciones:	Aprobar o rechazar las solicitudes de los académicos registrados al proceso de certificación de ANFECA.
Obligaciones:	Mantener confidencialidad de la información de los académicos y emplearla para el proceso de certificación que otorga la ANFECA.

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	**FCASIPCA01**
(Nombre del sistema A17)	Sistema de información del proceso de certificación de ANFECA
Tipo de soporte:	El soporte es electrónico y vía telefónica.
Descripción:	Base de datos relacional
Características del lugar donde se resguardan los soportes:	Sitio dentro del Centro de Informática de la FCA ubicado en la planta baja, cuenta con aire acondicionado a 18° centígrados, el acceso es con puerta de marco laminado y con vidrio, cuenta con una cerradura sencilla, la llave y la copia es manejada por el Administrador de Servidores y el jefe del Centro de Informática.

ANÁLISIS DE RIESGOS

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPCA01	
(Nombre del sistema A17)	Sistema de información del proceso de certificación académica de ANFECA[43]	
Riesgo	**Impacto**	**Mitigación**

[43] T**exto eliminado:** Apartado correspondiente a "Análisis de Riesgos" (página 183). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

ANÁLISIS DE BRECHA

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPCA01	
(Nombre del sistema A17)	Sistema de información del proceso de certificación académica de ANFECA.	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]

PLAN DE TRABAJO

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIPCA01
(Nombre del sistema A17)	Sistema de información del proceso de certificación académica de ANFECA.

[44] **Texto eliminado:** Apartado correspondiente a “Análisis de Riesgos, de Análisis de Brecha y del Plan de Trabajo” (páginas 184 a 185). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Actividad	Descripción	Duración	Cobertura
[redacted]	[redacted]	[redacted]	[redacted]

MEDIDAS DE SEGURIDAD IMPLEMENTADAS

TRANSFERENCIAS DE DATOS PERSONALES

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)	
Identificador único	FCASIPCA01
(Nombre del sistema A17)	Sistema de información del proceso de certificación académica de ANFECA.
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica, no se reciben documentos o expedientes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No aplica, no se intercambian archivos electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	La transferencia de la información es por medio de una red pública y se considera posteriormente incluir red privada virtual (VPN).

RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

El acceso al centro de datos y servidores es con llave y la chapa es sencilla, existe equipo de refrigeración que mantiene la temperatura a 18°, no existe un mecanismo para detección o supresión de incendios y cuenta con planta de luz y UPS.

Nombre	Cargo	Funciones	Obligaciones

[45] T**exto eliminado:** Apartado correspondiente a “Plan de Trabajo” (página 185). **Fundamento legal y motivación:** 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, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Mtro. Balfred Santaella Hinojosa	Jefe del Centro de Informática	Planeación, organización y control de los sistemas de información de la Facultad.	Asegurar el funcionamiento de los sistemas y servicios de información.
Mtro. Germán Ignacio Cervantes González	Administrador de Servidores	Gestión, configuración, mantenimiento y soporte de los servidores y las bases de datos.	Revisar y mantener la correcta operación y disponibilidad de los servicios que dan soporte a los distintos sistemas de información.

BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**
   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   No se registran bitácoras en el sistema, se emplean los logs del servidor.

   b) Para soportes físicos: Número o clave del expediente utilizado, y
   No aplica.

   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
   No aplica.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
   Los logs del servidor como soporte electrónico.
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
   En el sistema operativo de red de manera semanal.
4. La manera en que asegura la integridad de las bitácoras, y
   Con respaldos semanales.
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
   Administrador de servidores.
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
   No hay herramientas de análisis.

REGISTRO DE INCIDENTES

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   Germán Ignacio Cervantes Gonzáles (Servidores) y/o Hugo Díaz García (Responsable del sistema)
   b) La metodología aplicada;
      i. Se genera un informe con los daños ocurridos y el equipo faltante en el centro de datos, a partir de que se pueda acceder a las instalaciones se genera una lista de los servidores dañados junto con los sistemas que se ven afectados y el inventario

del equipo.

ii. Del incidente se toman fotografías y se genera un acta por el o la abogad(a) de la facultad con el fin de denunciar los hechos ante el ministerio público, se informará al abogado general de UNAM y autoridades universitarias acerca de las afectaciones.

iii. Durante no más a 5 días naturales de ocurrido el incidente se hace pública la denuncia y es publicada en la página de la FCA informando a la comunidad de los hechos, así como del robo y/o daño de la información sustraída.

iv. En el caso de robo de datos personales se alertará a los titulares por medio de un correo masivo del evento para que tomen sus precauciones acerca del uso indebido de los datos personales.

v. En el caso de un ataque externo se le informa del incidente a la DGTIC para que se tomen medidas correctivas y precautorias.

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y

d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

Del incidente se revisa el servidor y los respaldos para conocer que se puede recuperar y que se debe reinstalar y restaurar.

2. Si el registro está en soporte físico o en soporte electrónico;

El registro esta en soporte electrónico.

3. Cómo asegura la integridad de dicho registro, y

Empleando un MD5 y revisando los últimos índices de las principales tablas.

4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

Mtro. Balfred Santaella Hinojosa (Jefe del Centro de Informática)

ACCESO A LAS INSTALACIONES

Seguridad perimetral exterior (las instalaciones del área universitaria):

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado.

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

Puertas con chapas, vigilancia las 24 horas, sistema de circuito cerrado y alarma en los accesos principales.

PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?

No

b) ¿Es discrecional (matriz de control de acceso)?
No

c) ¿Está basado en roles (perfiles) o grupos?
Sí

d) ¿Está basado en reglas?
No

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Sí

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Sí

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Sí

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
No

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Administrador (Encargado) del sistema

b) ¿Quién autoriza la creación de nuevos perfiles?
Administrador (Encargado) del sistema

c) ¿Se lleva registro de la creación de nuevos perfiles?
No

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Sí

c) ¿Cómo se evita el acceso remoto no autorizado?
Firewall con iptables

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   - **a)** Completos_X_, diferenciales ___ o incrementales___;
   - **b)** De forma automática ____ o Manual __X___,
   - **c)** Periodicidad con que los realiza: ___semanal____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Discos duros

3. Cómo y dónde archiva esos medios, y
   Arreglos de discos
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Administrador de servidores

PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   No se cuenta con plan de contingencia, pero se planea desarrollarlo.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   No aplica.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);
   b) Si el sitio es propio o subcontratado con un tercero;
   c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
   d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.
   No aplica.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPCA01	
(Nombre del sistema A17)	Sistema de información del proceso de certificación de ANFECA	
Recurso	**Descripción**	**Control**
NANGIOS	Monitorea los recursos y servicios de los servidores.	Lo lleva a cabo el administrador de servidores Licencias de software libre

Procedimiento para la revisión de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPCA01	
(Nombre del sistema A17)	Sistema de información del proceso de certificación de ANFECA	
Medida de seguridad	**Procedimiento**	**Responsable**
No aplica.	*No aplica*	*No aplica*

Resultados de la evaluación y pruebas a las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPCA01	
(Nombre del sistema A17)	Sistema de información del proceso de certificación de ANFECA	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No aplica	*No aplica*	*No aplica*

Acciones para la corrección y actualización de las medidas de seguridad

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPCA01	
(Nombre del sistema A17)	Sistema de información del proceso de certificación de ANFECA	
Medida de seguridad	**Acciones**	**Responsable**
No aplica	*No aplica*	*No aplica*

PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIPCA01		
(Nombre del sistema A17)	Sistema de información del proceso de certificación académica de la ANFECA		
Actividad	**Descripción**	**Duración**	**Cobertura**
La capacitación se recibe a través de los cursos que se programan en la Unidad de transparencia y la DGTIC	*En línea, presencial y autogestión*	*Depende del programa de cada curso/taller designado por la dependencia a cargo de la impartición*	*Dependencias de la UNAM*

Programa de difusión de la protección a los datos personales

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIPCA01		
(Nombre del sistema A17)	Sistema de información del proceso de certificación de ANFECA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Incluir el enlace al aviso de privacidad	Se realiza de manera electrónica	Permanente	Usuarios del sistema

MEJORA CONTINUA

Actualización y mantenimiento de sistemas de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIPCA01		
(Nombre del sistema A17)	Sistema de información del proceso de certificación de ANFECA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Apegarse a los cambios que se lleven a cabo en el aviso de privacidad	*Actualizar el acceso de manera electrónica a la versión más reciente del aviso de privacidad vigente*	*Permanente*	*Usuarios del sistema*

Actualización y mantenimiento de equipo de cómputo

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)			
Identificador único	FCASIPCA01		
(Nombre del sistema A17)	Sistema de información del proceso de certificación de ANFECA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Instalación de parches de seguridad	Se descargan e instalan de manera manual	Cada que se recibe notificación de un nuevo parche de seguridad	Mantener la integridad de los datos ante amenazas
Limpieza de logs	Se elimina información histórica de bitácoras	Mensual	Ayuda a liberar espacio de almacenamiento

Procesos para la conservación, preservación y respaldos de información

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPCA01	
(Nombre del sistema A17)	Sistema de información del proceso de certificación de ANFECA	
Proceso	**Descripción**	**Responsable**
Se almacena la información en arreglos de discos de manera semanal	*Se copia la información del servidor al arreglo de discos* *Se rotan los respaldos previos para dar entrada a los siguientes* *Copiar un nuevo respaldo*	*Administrador de servidores* *Mtro. Germán Ignacio Cervantes González*

Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Centro de Informática de la Facultad de Contaduría y Administración (CIFCA)		
Identificador único	FCASIPCA01	
(Nombre del sistema A17)	Sistema de información del proceso de certificación académica de la ANFECA	
Proceso	**Descripción**	**Responsable**
Formateo a bajo nivel	Se realiza el formateo de bajo nivel a todos los discos	Administrador de servidores *Mtro. Germán Ignacio Cervantes González*

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

No se cuenta con un procedimiento, pero se planea desarrollarlo

APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

Responsable del desarrollo:	Mtro. Hugo Díaz García. Jefe de Sistemas. 56 23 70 00 ext 46248. Correo: hdiaz@fca.unam.mx Mtro. Raúl Esteban Cruz Quiroz. Responsable de Infraestructura. Tel. 56 23 70 00 ext 46244. Correo: rcruz@fca.unam.mx Dra. Adriana García Vargas. Responsable del Laboratorio de Cómputo. Tel. 56 23 70 00 ext 46845. Correo: agarcia@fca.unam.mx
Revisó:	Lic. Alberto García Pantoja. Enlace de Transparencia. 56 22 83 70 ext 111 algarcia@fca.unam.mx Mtro. Bernardo Alid Espinoza Urzua. Gestión de Indicadores Institucionales de la Secretaría de Planeación. Tel. 56 22 83 70 ext 111. Correo: bespinoza@fca.unam.mx
Autorizó:	Dr. Armando Tomé González. Secretario General de la FCA UNAM. Tel. 55 50 61 74; 56 22 83 72 y; 56 22 83 77 Correo: atome@fca.unam.mx
Fecha de aprobación:	
Fecha de actualización:	11 de enero de 2024.