CENTRO DE CIENCIAS MATEMÁTICAS

Documento de Seguridad de Datos Personales

Enero 2024

Documento de Seguridad de Datos Personales

Tabla de contenido

Introducción

El presente documento de seguridad contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales del **Centro de Ciencias Matemáticas (CCM)**, 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.

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

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

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Sistema Institucional de Compras

Bienes y Suministros	
Identificador único*	ByS-SIC
(Nombre del sistema A1) *	Sistema Institucional de Compras
Datos personales (sensibles o no) contenidos en el sistema*:	• *Nombres* • *Domicilios* • *Teléfonos Fijos* • *Teléfonos Particulares* • *Correo Electrónico* • *CURP* • *RFC*
Responsable*:	M.A. Adriana Briseño Chávez
Nombre*:	*M.A. Adriana Briseño Chávez*
Cargo*:	*Delegada Administrativa*
Funciones*:	• *Autorizaciones de Compras* • *Asignación de Suficiencias Presupuestales* • *Notificaciones ante DGPU* • *Generar Pagos*
Obligaciones*:	*Administrar y fiscalizar recursos financieros*
	Encargados:
(Nombre del Encargado 1*)	*L.C. Hermelidia Santibáñez Núñez*
Cargo*:	*Jefa de Área de Bienes y Suministros*
Funciones*:	• *Registrar Solicitudes Internas* • *Generar Pedidos* • *Recabar Firmas de los Proveedores sobre las Solicitudes de Compras* • *Subir las Solicitudes de Compras Firmadas* • *Recabar Firmas de los Vales de Entrega* • *Subir los Vales de Entrega Firmados* • *Subir Facturas*
Obligaciones*:	*Implementación de controles que permitan el correcto funcionamiento del área de compras, así como recabar toda la documentación soporte*
	Usuarios:
(Nombre del Usuario 1*)	*Luis Abel Castorena Martínez*
Cargo*:	*Titular de la Dependencia*
Funciones*:	*Autorización de Compras*

Obligaciones*:	*Supervisar la correcta aplicación de recursos*
(Nombre del Usuario 2*)	*Adriana Briseño Chávez*
Cargo*:	*Delegada Administrativa*
Funciones*:	• *Autorizaciones de Compras* • *Asignación de Suficiencias Presupuestales* • *Notificaciones ante DGPU* • *Generar Pagos*
Obligaciones*:	*Administrar y fiscalizar recursos financieros*
(Nombre del Usuario 3*)	*Hermelidia Santibáñez Núñez*
Cargo*:	*Jefa de Área de Bienes y Suministros*
Funciones*:	• *Registrar Solicitudes Internas* • *Generar Pedidos* • *Recabar Firmas de los Proveedores sobre las Solicitudes de Compras* • *Subir las Solicitudes de Compras Firmadas* • *Recabar Firmas de los Vales de Entrega* • *Subir los Vales de Entrega Firmados* • *Subir Facturas*
Obligaciones*:	*Implementación de controles que permitan el correcto funcionamiento del área de compras, así como recabar toda la documentación soporte*

Sistema Integral de Personal, expediente físico

Unidad Administrativa	
Identificador único*	**UA-1**
(Nombre del sistema A1) *	Sistema Integral de Personal. Expediente Físico
Datos personales (sensibles o no) contenidos en el sistema*:	*Datos sensibles y no sensibles* *1. Datos personales:* • *Nombre* • *Domicilio* • *Telefono particular* • *Correo electrónico* • *Estado civil* • *Sexo* • *Fecha de nacimiento* • *Edad* • *Nacionalidad* • *Firma* • *Registro Federal de Contribuyentes* • *Clave Unica de Registro de Población* • *Grado académico* • *Dependientes económicos* • *Nombre dirección, fecha de nacimiento, beneficiarios de seguro de vida, pago de marcha* • *Fotografía* • *Número de seguridad social*

	2. Datos Laborales: • *Curriculum* • *Número de expediente o empleado* • *Fecha de ingreso al CCM* • *Trayectoria laboral dentro del CCM* • *Nombramiento vigente* • *Antigüedad laboral dentro de la UNAM* • *Número de registro de la plaza ocupada* • *Area específica de conocimiento o de adscripcion* • *Comisiones oficiales o licencias con o sin goce de sueldo* • *Numero de horas prácticas y número de horas téoricas* • *Salario* • *Documentos de capacitación* *3. Datos patrimoniales:* • *Estado de cuenta financiero de la cuenta bancaria en la que se deposita la nómina del trabajador* • *Aviso de otro empleador* *4. Datos de tránsito y movimiento migratorios* • *Situación migratoria* *5. Datos personales sensibles:* • *Licencias médicas emitidas por el ISSSTE* • *Dictámenes médicos*
Responsable*:	**Delegación Administrativa**
Nombre*:	*Adriana Briseño Chávez*
Cargo*:	*Delegada Administrativa*
Funciones*:	*Recabar la documentación que contenga la información de cada trabajador adscrito al CCM*
Obligaciones*:	*-Implementar controles necesarios para proteger los datos personales de los trabajadores adscritos al CCM* *-Tomar medidas tendientes a asegurar la confidencialidad, integridad y disponibilidad de los datos personales de los trabajadores adscritos al CCM.* *- Contar con un usuario y contraseña seguros*
	Encargados:
(Nombre del Encargado 1*)	*Adriana Briseño Chávez*
Cargo*:	*Delegada Administrativa*
Funciones*:	*Recabar la documentación que contenga la información de cada trabajador adscrito al CCM*
Obligaciones*:	*-Implementar controles necesarios para proteger los datos personales de los trabajadores adscritos al CCM* *-Tomar medidas tendientes a asegurar la confidencialidad, integridad y disponibilidad de los datos personales de los trabajadores adscritos al CCM.* *- Contar con un usuario y contraseña seguros*

Expediente físico de Becarios Posdoctorales

Unidad Administrativa	
Identificador único*	**UA-2**
(Nombre del sistema A1) *	Expediente Físico de Becarios Posdoctorales
Datos personales (sensibles o no) contenidos en el sistema*:	*Datos sensibles y no sensibles* *1. Datos personales:* • *Nombre* • *Domicilio* • *Telefono particular* • *Correo electrónico* • *Estado civil* • *Sexo* • *Fecha de nacimiento* • *Edad* • *Nacionalidad* • *Firma* • *Registro Federal de Contribuyentes* • *Clave Unica de Registro de Población* • *Grado académico* • *Dependientes económicos* • *Nombre dirección, fecha de nacimiento, beneficiarios de seguro de vida, pago de marcha* • *Fotografía* *2. Datos Laborales:* • *Curriculum* • *Documentos de capacitación* *3. Datos patrimoniales:* • *Estado de cuenta financiero de la cuenta bancaria* • *Aviso de otro empleador* *4. Datos de tránsito y movimiento migratorios* • *Situación migratoria*
Responsable*:	**Delegación Administrativa**
Nombre*:	*Adriana Briseño Chávez*
Cargo*:	*Delegada Administrativa*
Funciones*:	*Recabar la documentación que contenga la información de cada becario posdoctoral*
Obligaciones*:	*-Implementar controles necesarios para proteger los datos personales de los becarios posdoctorales* *-Tomar medidas tendientes a asegurar la confidencialidad, integridad y disponibilidad de los datos personales*
	Encargados:
(Nombre del Encargado 1*)	*Adriana Briseño Chávez*
Cargo*:	*Delegada Administrativa*
Funciones*:	*Recabar la documentación que contenga la información de cada becario posdoctoral*
Obligaciones*:	*-Implementar controles necesarios para proteger los datos personales de los becarios posdoctorales*

	-Tomar medidas tendientes a asegurar la confidencialidad, integridad y disponibilidad de los datos personales

Expediente Físico de Prestadores de Servicios Profesionales

Unidad Administrativa	
Identificador único*	**UA-3**
(Nombre del sistema A1) *	Expediente Físico de Prestadores de Servicios Profesionales
Datos personales (sensibles o no) contenidos en el sistema*:	*Datos sensibles y no sensibles* *1. Datos personales:* • *Nombre* • *Domicilio* • *Telefono particular* • *Correo electrónico* • *Sexo* • *Fecha de nacimiento* • *Edad* • *Nacionalidad* • *Firma* • *Registro Federal de Contribuyentes* • *Clave Unica de Registro de Población* • *Grado académico* *2. Datos Laborales:* • *Curriculum* • *Área específica de conocimiento* • *Salario* • *Documentos de capacitación* *3. Datos patrimoniales:* • *Estado de cuenta financiero de la cuenta bancaria en la que se deposita la nómina del trabajador* • *Aviso de otro empleador* *4. Datos de tránsito y movimiento migratorios* • *Situación migratoria*
Responsable*:	**Delegación Administrativa**
Nombre*:	*Adriana Briseño Chávez*
Cargo*:	*Delegada Administrativa*
Funciones*:	*Recabar la documentación que contenga la información*
Obligaciones*:	*-Implementar controles necesarios para proteger los datos personales* *-Tomar medidas tendientes a asegurar la confidencialidad, integridad y disponibilidad de los datos personales*
	Encargados:
(Nombre del Encargado 1*)	*Adriana Briseño Chávez*
Cargo*:	*Delegada Administrativa*
Funciones*:	*Recabar la documentación que contenga la información*
Obligaciones*:	*-Implementar controles necesarios para proteger los datos personales*

	-Tomar medidas tendientes a asegurar la confidencialidad, integridad y disponibilidad de los datos personales

Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT

Unidad Administrativa	
Identificador único*	**UA-4**
(Nombre del sistema A1) *	Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT
Datos personales (sensibles o no) contenidos en el sistema*:	*Datos sensibles y no sensibles* *1. Datos personales:* • *Nombre* • *Domicilio* • *Telefono particular* • *Correo electrónico* • *Sexo* • *Fecha de nacimiento* • *Edad* • *Nacionalidad* • *Firma* • *Registro Federal de Contribuyentes* • *Clave Unica de Registro de Población* • *Fotografía* • *INE* *2. Datos Laborales:* • *Curriculum* • *Monto de beca* *3. Datos patrimoniales:* • *Estado de cuenta financiero de la cuenta bancaria* *4. Datos de tránsito y movimiento migratorios* • *Situación migratoria* *5. Datos académicos* • *Historial académico* • *Constancia de estudios* • *Grado académico*
Responsable*:	**Delegación Administrativa**
Nombre*:	*Adriana Briseño Chávez*
Cargo*:	*Delegada Administrativa*
Funciones*:	*Recabar la documentación que contenga la información de cada trabajador adscrito al CCM* *Alimentar los sistemas informáticos institucionales para actualizar distintos proyectos.*
Obligaciones*:	*- Implementar controles necesarios para proteger los datos personales* *- Tomar medidas tendientes a asegurar la confidencialidad, integridad y disponibilidad de los datos personales* *- Resguardar la documentación y mantenerla actualizada e integrada por proyecto*

	Encargados:
(Nombre del Encargado 1*)	*Adriana Briseño Chávez*
Cargo*:	*Delegada Administrativa*
Funciones*:	*Recabar la documentación que contenga la información de cada trabajador adscrito al CCM* *Alimentar los sistemas informáticos institucionales para actualizar distintos proyectos.*
Obligaciones*:	*- Implementar controles necesarios para proteger los datos personales* *- Tomar medidas tendientes a asegurar la confidencialidad, integridad y disponibilidad de los datos personales* *- Resguardar la documentación y mantenerla actualizada e integrada por proyecto*

Sistema para la Administración de Asuntos Académico-Administrativos

Secretaría Académica	
Identificador único*	**SA-1**
(Nombre del sistema A1) *	Sistema para la Administración de Asuntos Académico-Administrativos
Datos personales (sensibles o no) contenidos en el sistema*:	*1. Datos de identificación:* • *Nombre completo* • *RFC* *2. Datos laborales:* • *Entidad de adscripción* • *Licencias* • *Comisiones* • *Promociones* • *Renovación de contrato* • *Definitividad* *3. Datos académicos:* • *Categoría* • *Número de empleado*
Responsable*:	**Consejo Técnico de la Investigación Científica. Centro de Ciencias Matemáticas. Secretaría Académica.**
Nombre*:	*José Ferrán Valdez Lorenzo*
Cargo*:	*Secretario Académico*
Funciones*:	*Recepción de solicitudes de licencia, comisiones, visitantes. Trámites de promoción, contratación, recontratación, definitividad, cambios de adscripción*
Obligaciones*:	*Presentar ante el Consejo Interno asuntos académicos-administrativos. Obtener la ratificación del Consejo Técnico*
	Encargados:
(Nombre del Encargado 1*)	*Valdemar Orozco Cárdenas*
Cargo*:	*Auxiliar de la Secretaría Académica*

Funciones*:	*Recepción de solicitudes de licencia, comisiones, visitantes. Trámites de promoción, contratación, recontratación, definitividad, cambios de adscripción.*
Obligaciones*:	*Presentar ante el Consejo Interno asuntos académicos-administrativos. Obtener la ratificación del Consejo Técnico.*

Sistema de Información Académica

Secretaría Académica	
Identificador único*	**SA-2**
Sistema (Nombre del A2)*:	Sistema de Información Académica
Datos personales contenidos en el sistema*:	• *Nombre del trabajador*
Responsable*:	**Secretaría Académica**
Nombre*:	*José Ferrán Valdez lorenzo*
Cargo*:	*Secretario Académico*
Funciones*:	*Recepción de solicitudes de licencia, comisiones, visitantes. Trámites de promoción, contratación, recontratación, definitividad, cambios de adscripción.*
Obligaciones*:	*Presentar ante el Consejo Interno asuntos académicos-administrativos. Obtener la ratificación del Consejo Técnico.*
	Encargados:
(Nombre del Encargado 1*)	*Valdemar Orozco Cárdenas*
Cargo*:	*Auxiliar de la Secretaría Académica*
Funciones*:	*Recepción de solicitudes de licencia, comisiones, visitantes. Trámites de promoción, contratación, recontratación, definitividad, cambios de adscripción.*
Obligaciones*:	*Presentar ante el Consejo Interno asuntos académicos-administrativos.*

Sistema de ingreso para alumnos de posgrado

Coordinación Administrativa del Posgrado de Matemáticas	
Identificador único*	PCCM-1
(Nombre del sistema A1) *	Sistema de ingreso para alumnos de posgrado
Datos personales (sensibles o no) contenidos en el sistema*:	*Datos de identificación:* • *Nombres* • *Domicilios* • *Teléfonos Fijos* • *Teléfonos Particulares* • *Correo Electrónico* • *CURP*

	• *RFC*
Responsable*:	DGAE UNAM
Nombre*:	
Cargo*:	
Funciones*:	• *Registro de aspirantes al posgrado, seguimiento de aspirantes*
Obligaciones*:	
	Encargados:
(Nombre del Encargado 1*)	
Cargo*:	
Funciones*:	
Obligaciones*:	
	Usuarios:
(Nombre del Usuario 1*)	*Morelia Ibone Alvarez Llanes*
Cargo*:	*Jefe de Área*
Funciones*:	*Dar seguimiento a alumnos, ingreso, permanencia y grado*
Obligaciones*:	*Revisión y monitoreo de información presentada en el sistema únicamente para uso informativo y de reportes, el área no cuenta con privilegios de acceso para manipulación y modificación de datos personales*

Sistema Integral de Administración Escolar del Posgrado (SIAE-P)

Coordinación Administrativa del Posgrado de Matemáticas	
Identificador único*	PCCM-2
(Nombre del sistema A1) *	Sistema Integral de Administración Escolar del Posgrado (SIAE-P)
Datos personales (sensibles o no) contenidos en el sistema*:	*Datos de identificación:* • *Nombres* • *Domicilios* • *Teléfonos Fijos* • *Teléfonos Particulares* • *Correo Electrónico* • *CURP* • *RFC*
Responsable*:	DGAE UNAM
Nombre*:	
Cargo*:	
Funciones*:	• *Captura de datos para seguimiento de alumnos, ingreso, permanencia y grado*
Obligaciones*:	

	Encargados:
(Nombre del Encargado 1*)	
Cargo*:	
Funciones*:	
Obligaciones*:	
	Usuarios:
(Nombre del Usuario 1*)	*Morelia Ibone Alvarez Llanes*
Cargo*:	*Jefe de Área*
Funciones*:	*Dar seguimiento a alumnos, ingreso, permanencia y grado*
Obligaciones*:	*Revisión y monitoreo de información presentada en el sistema únicamente para uso informativo y de reportes, el área no cuenta con privilegios de acceso para manipulación y modificación de datos personales*

Sistema Integral de Automatización de Bibliotecas Koha

Unidad de Documentación - Biblioteca	
Identificador único*	UDB-1
(Nombre del sistema A1) *	Sistema Integral de Automatización de Bibliotecas Koha
Datos personales (sensibles o no) contenidos en el sistema*:	• *Nombre completo* • *Fecha de Nacimiento* • *Género* • *Domicilio* • *Teléfono* • *Dirección Alternativa* • *Correo electrónico* • *Contacto alternativo* • *Número de credencial* • *Tipo de usuario* • *Fecha de Registro y de vencimiento* • *RFC* • *CURP*
Responsable*:	Dirección General de Bibliotecas y Servicios Digitales de Información
Nombre*:	*No aplica*
Cargo*:	*No aplica*
Funciones*:	*No aplica*
Obligaciones*:	*Las establecidas en los Lineamientos para la Protección de Datos Personales en posesión de la UNAM para responsables del tratamiento de datos personales en las áreas universitarias.*
	Encargados:
(Nombre del Encargado*)	*No aplica*
Cargo*:	*No aplica*
	Usuarios:
(Nombre del Usuario 1*)	*Lidia González García*
Cargo*:	*Técnica Académica*

Funciones*:	*Se recaban datos personales para el regstro en los sistemas de biblioteca que permite el acceso, préstamo remoto y físico de recursos de información tanto en formato impreso o digital.*
Obligaciones*:	*Llevar un registro de los usuarios a los cuales se les brindan los servicios y productos de información de biblioteca.* *Procurar la privacidad de los datos personales a los que accede mediante el uso del sistema.*
(Nombre del Usuario 2*)	*Juan Alejandro Medina Alanis*
Cargo*:	*Técnico Académico*
Funciones*:	*Se recaban datos personales para el regstro en los sistemas de biblioteca que permite el acceso, préstamo remoto y físico de recursos de información tanto en formato impreso o digital.*
Obligaciones*:	*Llevar un registro de los usuarios a los cuales se les brindan los servicios y productos de información de biblioteca.* *Procurar la privacidad de los datos personales a los que accede mediante el uso del sistema.*

Formato de Registro de Usuarios de la Biblioteca

Unidad de Documentación - Biblioteca	
Identificador único*	UDB-2
(Nombre del sistema A1) *	*Formato de Registro de Usuarios de la Biblioteca*
Datos personales (sensibles o no) contenidos en el sistema*:	• *Nombre Completo* • *Número de Cuenta* • *RFC* • *Domicilio* • *Correo Electrónico* • *Firma del aval de Biblioteca.*
Responsable*:	*Unidad de Documentación*
Nombre*:	*Lidia González García*
Cargo*:	*Técnica Académica*
Funciones*:	*Se recaban datos personales para el registro en los sistemas de biblioteca que permite el acceso y préstamo de recursos de información tanto en formato impreso como digital.*
Obligaciones*:	*Llevar un registro de los usuarios a los cuales se les brinda los servicios y productos de información de biblioteca.*
	Encargados:
(Nombre del Encargado 1*)	*Lidia González García*
Cargo*:	*Técnica Académica*
Funciones*:	*Se recaba información para el registro en los sistemas de biblioteca que permite el acceso y préstamo de recursos de información tanto en formato impreso como digital.*

(Nombre del Encargado 2*)	*Juan Alejandro Medina Alanis*
Cargo*:	*Técnico Académico*
Funciones*:	*Se recaba información para el registro en los sistemas de biblioteca que permite el acceso y préstamo de recursos de información tanto en formato impreso como digital.*
Obligaciones*:	*Llevar un registro de los usuarios a los cuales se les brinda los servicios y productos de información de biblioteca.*
	Usuarios:
(Nombre del Usuario 1*)	*Lidia González García*
Cargo*:	*Técnica Académica*
Funciones*:	*Se recaban datos personales para el registro en los sistemas de biblioteca que permite el acceso, préstamo remoto y físico de recursos de información tanto en formato impreso o digital.*
Obligaciones*:	*Llevar un registro de los usuarios a los cuales se les brindan los servicios y productos de información de biblioteca.* *Procurar la privacidad de los datos personales a los que accede mediante el uso del sistema.*
(Nombre del Usuario 2*)	*Juan Alejandro Medina Alanis*
Cargo*:	*Técnico Académico*
Funciones*:	*Se recaban datos personales para el registro en los sistemas de biblioteca que permite el acceso, préstamo remoto y físico de recursos de información tanto en formato impreso o digital.*
Obligaciones*:	*Llevar un registro de los usuarios a los cuales se les brindan los servicios y productos de información de biblioteca.* *Procurar la privacidad de los datos personales a los que accede mediante el uso del sistema.*

Sistema de Registro para Participación en Eventos del CCM

Unidad de Docencia	
Identificador único*	UDC-1
(Nombre del sistema A1) *	Sistema de Registro para Participación en Eventos del CCM
Datos personales (sensibles o no) contenidos en el sistema*:	*Datos de identificación:* • *Nombre* • *Domicilio* • *Teléfono celular* • *Correo electrónico* • *Firma* • *RFC* • *CURP* • *Lugar de nacimiento* • *Fecha de nacimiento*

	• *Nacionalidad* • *Edad* • *Nombres de familiares* • *Dependientes y beneficiarios* *Datos laborales:* • *Documentos de nombramiento* • *Documentos de capacitación* • *Referencias laborales* • *Referencias personales*
Responsable*:	*Centro de Ciencias Matemáticas*
Nombre*:	*Noé Bárcenas Torres*
Cargo*:	*Coordinador de la Unidad de Docencia*
Funciones*:	*Decidir sobre el tratamiento automatizado de los datos personales, así como la finalidad y uso del sistema*
Obligaciones*:	*Las establecidas en los Lineamientos para la Protección de Datos Personales en posesión de la UNAM para responsables del tratamiento de datos personales en las áreas universitarias.*
	Encargados:
(Nombre del Encargado 1*)	*Luis Gerardo Tejero Gómez*
Cargo*:	*Técnico Académico*
Funciones*:	*Realizar el desarrollo de software a la medida de acuerdo a las necesidades del CCM y apoyándo técnicamente en los procesos definidos en las áreas internas.*
Obligaciones*:	*Implementar medidas, estrategias técnicas y de seguridad necesarias en el sistema para garantizar la protección de los datos personales solicitados.*
(Nombre del Encargado 2*)	*Miguel Ángel Magaña Lemus*
Cargo*:	*Técnico Académico*
Funciones*:	*Realizar el desarrollo de software a la medida de acuerdo a las necesidades del CCM y apoyándo técnicamente en los procesos definidos en las áreas internas.*
Obligaciones*:	*Implementar medidas, estrategias técnicas y de seguridad necesarias en el sistema para garantizar la protección de los datos personales solicitados.*
	Usuarios:
(Nombre del Usuario 1*)	*Naila Itzel Angelina Centeno*
Cargo*:	*Técnica Académica*
Funciones*:	*Organización de eventos académicos en distintos niveles educativos.*
Obligaciones*:	*Revisar las solicitudes para determinar quienes participan en dichos eventos.*

Formato de Seguros

Dirección	
Identificador único*	DIR-1
(Nombre del sistema A1) *	Formato de Seguros

Datos personales (sensibles o no) contenidos en el sistema*:	*Datos de identificación:* • *Nombre* • *RFC* • *CURP* • *Dependientes y beneficiarios*
Responsable*:	Centro de Ciencias Matemáticas
Nombre*:	*Jorge Alejandro Romero Rodríguez*
Cargo*:	*Asitente de Dirección*
Funciones*:	*Recabar firma y huella digital de interesado y envíar formatos vía correo electrónico a la Subdirección de Seguros de la UNAM*
Obligaciones*:	*Archivar formato físico*
	Encargados:
(Nombre del Encargado 1*)	*Jorge Alejandro Romero Rodríguez*
Cargo*:	*Asitente de Dirección*
Funciones*:	*Recabar firma y huella digital de interesado y envíar formatos vía correo electrónico a la Subdirección de Seguros de la UNAM*
Obligaciones*:	*Archivar formato físico*

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

Bienes y Suministros	
Identificador único¨*	ByS
(Nombre del sistema A1*)	Sistema Institucional de Compras
Tipo de soporte:*	*Soporte Físico y Electrónico*
Descripción:*	*Soportes físicos: expedientes impresos y archivados en carpetas.* *Soportes electrónicos: archivos PDF guardados en PC y en el sitio https://www.sic.unam.mx/*
Características del lugar donde se resguardan los soportes:*	*Soportes físicos: oficina con ventilación natural, luz natural y artificial, puerta de acceso de cristal y chapa, aislada de humedad, con archiveros y libreros que permiten la conservación adecuada de los documentos.* *Soportes electrónicos: archivos PDF guardados en PC de la Unidad Administrativa del CCM. El acceso a la información utiliza medidas de seguridad ofrecidas por el sistema operativo; y en el sitio https://www.sic.unam.mx/*

Unidad Administrativa	
Identificador único¨*	UA-1
(Nombre del sistema A1*)	Sistema Integral de Personal. Expediente
Tipo de soporte:*	*Soporte físico*
Descripción:*	*Expedientes*

Características del lugar donde se resguardan los soportes:*	*Archivero con cerradura* *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.*

Unidad Administrativa	
Identificador único¨*	UA-2
(Nombre del sistema A1*)	Expediente Físico de Becarios Posdoctorales
Tipo de soporte:*	*Soporte electrónico y físico.*
Descripción:*	*Expedientes físicos y electrónicos*
Características del lugar donde se resguardan los soportes:*	*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.*

Unidad Administrativa	
Identificador único¨*	UA-3
(Nombre del sistema A1*)	Expediente Físico de Prestadores de Servicios Profesionales
Tipo de soporte:*	*Soporte físico*
Descripción:*	*Expedientes físicos y electrónicos*
Características del lugar donde se resguardan los soportes:*	*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.*

Unidad Administrativa	
Identificador único¨*	UA-4
(Nombre del sistema A1*)	Expediente Físico de Poyectos PAPIIT, PAPIME y CONACYT
Tipo de soporte:*	*Soporte físico*
Descripción:*	*Expedientes*
Características del lugar donde se resguardan los soportes:*	*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.*

Secretaría Académica	
Identificador único¨*	SA-1
(Nombre del sistema A1*)	Sistema para la Administración de Asuntos Académico-Administrativos
Tipo de soporte:*	*Electrónico*
Descripción:*	*Base de datos*
Características del lugar donde se resguardan los soportes:*	*Alojamiento en la plataforma del CTIC*

Secretaría Académica	
Identificador único¨*	SA-2
(Nombre del sistema A1*)	Sistema de Información Académica
Tipo de soporte:*	*Electrónico*

Descripción:*	*Base de datos*
Características del lugar donde se resguardan los soportes:*	*El Sistema de Información Académica y su base de datos se encuentran en uno de los servidores dentro de la infraestructura del CCM. El acceso físico a los servidores del CCM se encuentra restringido por cerraduras, la Unidad de Cómputo del CCM es el único personal autorizado que tiene acceso a ellos. El servidor que contiene el Sistema de Información Académica y su base de datos, cuenta con medidas de seguridad implementadas por el sistema operativo del servidor, así como de herramientas que monitorizan los intentos de acceso al sistema. El acceso al sistema por parte de los usuarios es a través de un usuario y contraseña, la consulta o modificación de información está controlada por roles de usuario.*

Coordinación Administrativa del Posgrado de Matemáticas	
Identificador único¨*	PCCM-1
(Nombre del sistema A1*)	Sistema de ingreso para alumnos de posgrado
Tipo de soporte:*	*Electrónico*
Descripción:*	*Registro de alumnos aspirantes al posgrado*
Características del lugar donde se resguardan los soportes:*	*Alojamiento en la Dirección General de Administración Escolar*

Coordinación Administrativa del Posgrado de Matemáticas	
Identificador único¨*	PCCM-2
(Nombre del sistema A1*)	Sistema Integral de Administración Escolar del Posgrado
Tipo de soporte:*	*Electrónico*
Descripción:*	*Registro de alumnos del posgrado, cursos, tramites de grado, alta de profesores*
Características del lugar donde se resguardan los soportes:*	*Alojamiento en la Dirección General de Administración Escolar*

Unidad de Documentación - Biblioteca	
Identificador único¨*	UDB-1
(Nombre del sistema A1*)	Sistema Integral de Automatización de Biblioteca Koha
Tipo de soporte:*	*Soporte electrónico*
Descripción:*	*Base de datos*
Características del lugar donde se resguardan los soportes:*	*Alojamiento en el servidor virtual del Instituto de Investigaciones en Ecosistemas*

Unidad de Documentación - Biblioteca	
Identificador único¨*	UDB-2
(Nombre del sistema A2*)	Formato de Registro de Usuarios de la Biblioteca
Tipo de soporte*:	*Físico*
Descripción*:	*Expedientes*

Características del lugar donde se resguardan los soportes*:	*Oficina con ventilación natural, luz natural y artificial, puerta de acceso de madera y chapa, archivero y libreros que permiten la conservación adecuada de los documentos.*

Unidad de Docencia	
Identificador único¨*	UDC-1
(Nombre del sistema A1*)	Sistema de Registro para Participación en Eventos del CCM
Tipo de soporte:*	*Electrónico*
Descripción:*	*Base de datos*
Características del lugar donde se resguardan los soportes:*	*El Sistema de Registro para Participación en Eventos del CCM y su base de datos se encuentran en uno de los servidores dentro de la infraestructura del CCM. El acceso físico a los servidores del CCM se encuentra restringido por cerraduras, la Unidad de Cómputo del CCM es el único personal autorizado que tiene acceso a ellos. El servidor que contiene el Sistema de Información Académica y su base de datos, cuenta con medidas de seguridad implementadas por el sistema operativo del servidor, así como de herramientas que monitorizan los intentos de acceso al sistema. El acceso al sistema por parte de los usuarios es a través de un usuario y contraseña, la consulta o modificación de información está controlada por roles de usuario.* *Información de la base de datos se encuentra en archivos contenidos en una PC perteneciente a la Unidad de Docencia. La ubicación física de esta PC es en la oficina de la Unidad de Docencia la cual tiene un acceso restringido por una cerradura. El acceso a esta utiliza medidas de seguridad brindadas por el sistema operativo.*

Dirección	
Identificador único¨*	DIR-1
(Nombre del sistema A1*)	Formato de Seguros
Tipo de soporte:*	*Físico y electrónico*
Descripción:*	*Base de datos*
Características del lugar donde se resguardan los soportes:*	*Los formatos físicos se resguardan en archivero con llave.* *Información de la base de datos se encuentra en archivos contenidos en una PC perteneciente a la Dirección del CCM. La ubicación física de esta PC es en la Dirección la cual tiene un acceso restringido por una cerradura. El acceso a esta utiliza medidas de seguridad brindadas por el sistema operativo.*

3. ANÁLISIS DE RIESGOS

Bienes y Suministros		
Identificador único*	ByS	
(Nombre del sistema A1) *	Sistema Institucional de Compras	
Riesgo*	**Impacto***	**Mitigación***
Robo de archivos con expedientes	*Acceso a información que solo personal autorizado puede ver. Divulgación de información o mal uso de la misma.*	*Expedientes en archivero con cerradura y computadora con contraseña. Utilización de contraseñas robustas de mínimo 12 caracteres utilizando*

		combinaciones de letras, números, símbolos, mayúsculas, minúsculas.

Unidad Administrativa		
Identificador único*	UA-1	
(Nombre del sistema A1) *	Sistema Integral de Personal. Expediente Físico	
Riesgo*	**Impacto***	**Mitigación***
Robo de expedientes	*Acceso a información que solo personal autorizado puede ver. Divulgación de información o mal uso de la misma.*	*Expedientes en archivero con cerradura. Cierre de oficina con cerradura. Identificación del personal que accede al área donde se encuentra la información resguardada.*

Unidad Administrativa		
Identificador único*	UA-2	
(Nombre del sistema A1) *	Expediente Físico de Becarios Posdoctorales	
Riesgo*	**Impacto***	**Mitigación***
Robo de expedientes	*Acceso a información que solo personal autorizado puede ver. Divulgación de información o mal uso de la misma.*	*Expedientes en archivero con cerradura. Cierre de oficina con cerradura. Identificación del personal que accede al área donde se encuentra la información resguardada.*

Unidad Administrativa		
Identificador único*	UA-3	
(Nombre del sistema A1) *	Expediente Físico de Prestadores de Servicios Profesionales	
Riesgo*	**Impacto***	**Mitigación***
Robo de expedientes	*Acceso a información que solo personal autorizado puede ver. Divulgación de información o mal uso de la misma.*	*Expedientes en archivero con cerradura. Cierre de oficina con cerradura. Identificación del personal que accede al área donde se encuentra la información resguardada.*

Unidad Administrativa		
Identificador único*	UA-4	
(Nombre del sistema A1) *	Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT	
Riesgo*	**Impacto***	**Mitigación***
Robo de expedientes	*Acceso a información que solo personal autorizado puede ver. Divulgación de información o mal uso de la misma.*	*Expedientes en archivero con cerradura. Cierre de oficina con cerradura. Identificación del personal que accede al área donde se encuentra la información resguardada.*

Secretaría Académica		
Identificador único*	SA-1	
(Nombre del sistema A1) *	Sistema para la Administración de Asuntos Académico-Administrativos	
Riesgo*	**Impacto***	**Mitigación***

Uso de contraseñas débiles, contraseñas cortas fáciles de romper	*Acceso a información que solo personal autorizado puede ver. Divulgación de información o mal uso de la misma.*	*Utilización de contraseñas robustas de mínimo 12 caracteres utilizando combinaciones de letras, números, símbolos, mayúsculas, minúsculas.*

Secretaría Académica		
Identificador único*	SA-2	
(Nombre del sistema A1) *	Sistema de Información Académica	
Riesgo*	**Impacto***	**Mitigación***
Uso de contraseñas débiles, contraseñas cortas fáciles de romper	*Acceso a información que solo personal autorizado puede ver. Divulgación de información o mal uso de la misma.*	*Utilización de contraseñas robustas de mínimo 12 caracteres utilizando combinaciones de letras, números, símbolos, mayúsculas, minúsculas.*
Vulnerabilidades del framework con el que fue desarrollado el sistema	*Acceso no autorizado al sistema. Acceso a información que solo personal autorizado puede ver.*	*Actualización constante del framework y del lenguaje de programación para el que fue diseñado.*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-1	
(Nombre del sistema A1) *	Sistema de ingreso para alumnos de posgrado	
Riesgo*	**Impacto***	**Mitigación***
Uso de contraseñas débiles, contraseñas cortas fáciles de romper	*Acceso a información que solo personal autorizado puede ver. Divulgación de información o mal uso de la misma.*	*Utilización de contraseñas robustas de mínimo 12 caracteres utilizando combinaciones de letras, números, símbolos, mayúsculas, minúsculas.*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-2	
(Nombre del sistema A1) *	Sistema Integral de Administración Escolar del Posgrado	
Riesgo*	**Impacto***	**Mitigación***
Uso de contraseñas débiles, contraseñas cortas fáciles de romper	*Acceso a información que solo personal autorizado puede ver. Divulgación de información o mal uso de la misma.*	*Utilización de contraseñas robustas de mínimo 12 caracteres utilizando combinaciones de letras, números, símbolos, mayúsculas, minúsculas.*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-1	
(Nombre del sistema A1) *	Sistema Integral de Automatización de Bibliotecas Koha	
Riesgo*	**Impacto***	**Mitigación***

Uso de contraseñas débiles, contraseñas cortas fáciles de romper	*Acceso a información que solo personal autorizado puede ver. Divulgación de información o mal uso de la misma.*	*Utilización de contraseñas robustas de mínimo 12 caracteres utilizando combinaciones de letras, números, símbolos, mayúsculas, minúsculas.*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-2	
(Nombre del sistema A1) *	Formato de Registro de Usuarios de la Biblioteca	
Riesgo*	**Impacto***	**Mitigación***
Robo de archivos	*Acceso a información que solo personal autorizado puede ver. Divulgación de información o mal uso de la misma.*	*Expedientes en archivero con cerradura. Cierre de oficina con cerradura. Identificación del personal que accede al área donde se encuentra la información resguardada.*

Unidad de Docencia		
Identificador único*	UDC-1	
(Nombre del sistema A1) *	Sistema de Registro para Participación en Eventos del CCM	
Riesgo*	**Impacto***	**Mitigación***
Daño físico del servidor	*Perder la base de datos con información sobre la participación que se tiene en los eventos académicos del CCM.*	*Contar con una estrategia de respaldos y medidas para asegurar la disponibilidad de la información.*

Dirección		
Identificador único*	DIR-1	
(Nombre del sistema A1) *	Formato de Seguros	
Riesgo*	**Impacto***	**Mitigación***
Robo de archivos	*Acceso a información que solo personal autorizado puede ver. Divulgación de información o mal uso de la misma.*	*Expedientes en archivero con cerradura y computadora con contraseña. Utilización de contraseñas seguras de mínimo 12 caracteres utilizando combinaciones de letras, números, símbolos, mayúsculas, minúsculas.*

4. ANÁLISIS DE BRECHA

Bienes y Suministros		
Identificador único*	ByS	
(Nombre del sistema A1) *	Sistema Institucional de Compras	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Seguridad física, expedientes en archivero con cerradura y computadora con contraseña.	*Los expedientes se resguardarán en el mobiliario institucional y aquellos que contengan datos personales se*	*Siempre que el personal se ausente de su estación de trabajo, deberá bloquear las sesiones de sus equipos de cómputo.*

	preservarán con mecanismos idóneos. *Protección de los equipos de cómputo, mediante un bloqueo de pantalla o desconexión cuando no está en uso.*	*Todos los equipos de cómputo deberán tener configurado el bloqueo de sesión por inactividad.* *Siempre que el personal se ausente de su estación de trabajo deberá bloquear todos los equipos y dispositivos que de él dependen y/o utiliza.*

Unidad Administrativa		
Identificador único*	UA-1	
(Nombre del sistema A1) *	Sistema Integral de Personal. Expediente Físico	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Seguridad física, cierre de oficina y cajones.	*Establecer control físico de ingreso a las instalaciones, archivos y soportes físicos.* *Los expedientes se resguardarán en el mobiliario institucional y aquellos que contengan datos personales se preservarán con mecanismos idóneos.*	*Proteger el entorno físico del manejo, traslado, resguardo y acceso a los datos personales contenidos en los documentos de archivo generados y recibidos, así como de los recursos involucrados en su tratamiento, a fin de prevenir robos, daños, pérdidas, alteraciones, destrucción o su uso, acceso o tratamiento no autorizado, para garantizar su confidencialidad, integridad y disponibilidad.*
Unidad Administrativa		
Identificador único*	UA-2	
(Nombre del sistema A1) *	Expediente Físico Becarios Posdoctorales	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Seguridad física, cierre de oficina y cajones.	*Establecer control físico de ingreso a las instalaciones, archivos y soportes físicos.* *Los expedientes se resguardarán en el mobiliario institucional y aquellos que contengan datos personales se preservarán con mecanismos idóneos.*	*Proteger el entorno físico del manejo, traslado, resguardo y acceso a los datos personales contenidos en los documentos de archivo generados y recibidos, así como de los recursos involucrados en su tratamiento, a fin de prevenir robos, daños, pérdidas, alteraciones, destrucción o su uso, acceso o tratamiento no autorizado, para garantizar su confidencialidad, integridad y disponibilidad.*

Unidad Administrativa		
Identificador único*	UA-3	
(Nombre del sistema A1) *	Expediente Físico de Prestadores de Servicios Profesionales	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***

Seguridad física, cierre de oficina y cajones.	*Establecer control físico de ingreso a las instalaciones, archivos y soportes físicos.* *Los expedientes se resguardarán en el mobiliario institucional y aquellos que contengan datos personales se preservarán con mecanismos idóneos.*	*Proteger el entorno físico del manejo, traslado, resguardo y acceso a los datos personales contenidos en los documentos de archivo generados y recibidos, así como de los recursos involucrados en su tratamiento, a fin de prevenir robos, daños, pérdidas, alteraciones, destrucción o su uso, acceso o tratamiento no autorizado, para garantizar su confidencialidad, integridad y disponibilidad.*

Unidad Administrativa		
Identificador único*	UA-4	
(Nombre del sistema A1) *	Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Seguridad física, cierre de oficina y cajones.	*Establecer control físico de ingreso a las instalaciones, archivos y soportes físicos.* *Los expedientes se resguardarán en el mobiliario institucional y aquellos que contengan datos personales se preservarán con mecanismos idóneos.*	*Proteger el entorno físico del manejo, traslado, resguardo y acceso a los datos personales contenidos en los documentos de archivo generados y recibidos, así como de los recursos involucrados en su tratamiento, a fin de prevenir robos, daños, pérdidas, alteraciones, destrucción o su uso, acceso o tratamiento no autorizado, para garantizar su confidencialidad, integridad y disponibilidad.*

Secretaría Académica		
Identificador único*	SA-1	
(Nombre del sistema A1) *	Sistema para la Administración de Asuntos Académicos-Administrativos	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Protección general del CCM. En el CCM se cuentan con diferentes medidas de seguridad para la protección de servicios, software y hardware. A nivel de red se tiene en funcionamiento un firewall que permite el monitoreo constante de su uso. Para el servicio de correo se cuenta con un equipo dedicado para protección de las comunicaciones entre servidores y seguridad en las peticiones realizadas. Los servicios tecnológicos que brinda el CCM son constantemente monitoreados y actualizados. En los sistemas del CCM se cuenta con perfiles de seguridad asignados a través de identificación y autenticación. Se	*Uso de contraseñas seguras.*	*Cambiar a una contraseña que cumpla con las caracteríticas para ser segura, de mínimo 12 caracteres utilizando combinaciones de letras, números, símbolos, mayúsculas, minúsculas. Que sea única y utilizada solo para este sistema.*

hace uso de certificados de seguridad y las comunicaciones se establecen de forma cifrada. Se realizan copias de seguridad de información y configuración de los servicios en el CCM.		

Secretaría Académica		
Identificador único*	SA-2	
(Nombre del sistema A1) *	Sistema de Información Académica	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Protección general del CCM. En el CCM se cuentan con diferentes medidas de seguridad para la protección de servicios, software y hardware. A nivel de red se tiene en funcionamiento un firewall que permite el monitoreo constante de su uso. Para el servicio de correo se cuenta con un equipo dedicado para protección de las comunicaciones entre servidores y seguridad en las peticiones realizadas. Los servicios tecnológicos que brinda el CCM son constantemente monitoreados y actualizados. En los sistemas del CCM se cuenta con perfiles de seguridad asignados a través de identificación y autenticación. Se hace uso de certificados de seguridad y las comunicaciones se establecen de forma cifrada. Se realizan copias de seguridad de información y configuración de los servicios en el CCM.	*Protección de la información.* *Actualización a las últimas versiones de bibliotecas y frameworks utilizados en el desarrollo del sistema.*	*Creación de copias de seguridad de la base de datos.* *Revisar periódicamente los registros del sistema para detectar comportamientos anormales y acciones fallidas.*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-1	
(Nombre del sistema A1) *	Sistema de ingreso para alumnos de posgrado	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Protección general del CCM. En el CCM se cuentan con diferentes medidas de seguridad para la protección de servicios, software y hardware. A nivel de red se tiene en funcionamiento un firewall que permite el monitoreo constante de su uso. Para el servicio de correo se cuenta con un equipo dedicado para protección de las comunicaciones entre servidores y seguridad en las peticiones realizadas. Los servicios	*Uso de contraseñas seguras.*	*Cambiar a una contraseña que cumpla con las caracteríticas para ser segura, de mínimo 12 caracteres utilizando combinaciones de letras, números, símbolos, mayúsculas, minúsculas. Que sea única y utilizada solo para este sistema.*

tecnológicos que brinda el CCM son constantemente monitoreados y actualizados. En los sistemas del CCM se cuenta con perfiles de seguridad asignados a través de identificación y autenticación. Se hace uso de certificados de seguridad y las comunicaciones se establecen de forma cifrada. Se realizan copias de seguridad de información y configuración de los servicios en el CCM.		

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-2	
(Nombre del sistema A1) *	Sistema Integral de Administración Escolar del Posgrado	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Protección general del CCM. En el CCM se cuentan con diferentes medidas de seguridad para la protección de servicios, software y hardware. A nivel de red se tiene en funcionamiento un firewall que permite el monitoreo constante de su uso. Para el servicio de correo se cuenta con un equipo dedicado para protección de las comunicaciones entre servidores y seguridad en las peticiones realizadas. Los servicios tecnológicos que brinda el CCM son constantemente monitoreados y actualizados. En los sistemas del CCM se cuenta con perfiles de seguridad asignados a través de identificación y autenticación. Se hace uso de certificados de seguridad y las comunicaciones se establecen de forma cifrada. Se realizan copias de seguridad de información y configuración de los servicios en el CCM.	*Uso de contraseñas seguras.*	*Cambiar a una contraseña que cumpla con las caracteríticas para ser segura, de mínimo 12 caracteres utilizando combinaciones de letras, números, símbolos, mayúsculas, minúsculas. Que sea única y utilizada solo para este sistema.*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-1	
(Nombre del sistema A1) *	Sistema Integral de Automatización de Bibliotecas Koha	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Protección general del CCM. En el CCM se cuentan con diferentes medidas de seguridad para la protección de servicios, software y hardware. A nivel de red se tiene en	*Uso de contraseñas seguras.*	*Cambiar a una contraseña que cumpla con las caracteríticas para ser segura, de mínimo 12 caracteres utilizando combinaciones de letras, números, símbolos, mayúsculas, minúsculas. Que*

funcionamiento un firewall que permite el monitoreo constante de su uso. Para el servicio de correo se cuenta con un equipo dedicado para protección de las comunicaciones entre servidores y seguridad en las peticiones realizadas. Los servicios tecnológicos que brinda el CCM son constantemente monitoreados y actualizados. En los sistemas del CCM se cuenta con perfiles de seguridad asignados a través de identificación y autenticación. Se hace uso de certificados de seguridad y las comunicaciones se establecen de forma cifrada. Se realizan copias de seguridad de información y configuración de los servicios en el CCM.		*sea única y utilizada solo para este sistema.*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-2	
(Nombre del sistema A1) *	Formato de Registro de Usuarios de la Biblioteca	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Seguridad física, cierre de oficina y cajones.	*Establecer control físico de ingreso a las instalaciones, archivos y soportes físicos.* *Los expedientes se resguardarán en el mobiliario institucional y aquellos que contengan datos personales se preservarán con mecanismos idóneos.*	*Proteger el entorno físico del manejo, traslado, resguardo y acceso a los datos personales contenidos en los documentos de archivo generados y recibidos, así como de los recursos involucrados en su tratamiento, a fin de prevenir robos, daños, pérdidas, alteraciones, destrucción o su uso, acceso o tratamiento no autorizado, para garantizar su confidencialidad, integridad y disponibilidad.*

Unidad de Docencia		
Identificador único*	UDC-1	
(Nombre del sistema A1) *	Sistema de Registro para Participación en Eventos del CCM	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Protección general del CCM. En el CCM se cuentan con diferentes medidas de seguridad para la protección de servicios, software y hardware. A nivel de red se tiene en funcionamiento un firewall que permite el monitoreo constante de su uso. Para el servicio de correo se cuenta con un equipo dedicado para protección de las comunicaciones entre servidores y seguridad en las	*Protección de la información.* *Actualización a las últimas versiones de bibliotecas y frameworks utilizados en el desarrollo del sistema.*	*Creación de copias de seguridad de la base de datos.* *Revisar periódicamente los registros del sistema para detectar comportamientos anormales y acciones fallidas. Contar con respaldos de las bases de datos y con un programa de eliminación segura de información una vez que ha cumplido su función.*

peticiones realizadas. Los servicios tecnológicos que brinda el CCM son constantemente monitoreados y actualizados. En los sistemas del CCM se cuenta con perfiles de seguridad asignados a través de identificación y autenticación. Se hace uso de certificados de seguridad y las comunicaciones se establecen de forma cifrada. Se realizan copias de seguridad de información y configuración de los servicios en el CCM.		
Dirección		
Identificador único*	DIR-1	
(Nombre del sistema A1) *	Formato de Seguros	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
Seguridad física, expedientes en archivero con cerradura y computadora con contraseña.	*Los expedientes se resguardarán en el mobiliario institucional y aquellos que contengan datos personales se preservarán con mecanismos idóneos.* *Protección de los equipos de cómputo, mediante un bloqueo de pantalla o desconexión cuando no está en uso.*	*Siempre que el personal se ausente de su estación de trabajo, deberá bloquear las sesiones de sus equipos de cómputo.* *Todos los equipos de cómputo deberán tener configurado el bloqueo de sesión por inactividad.* *Siempre que el personal se ausente de su estación de trabajo deberá bloquear todos los equipos y dispositivos que de él dependen y/o utiliza.*

5. PLAN DE TRABAJO

Bienes y Suministros			
Identificador único*	ByS		
(Nombre del sistema A1) *	Sistema Institucional de Compras		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad Administrativa			
Identificador único*	UA-1		
(Nombre del sistema A1) *	Sistema Integral de Personal. Expediente Físico		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad Administrativa	
Identificador único*	UA-2

(Nombre del sistema A1) *	Expediente Físico de Becarios Posdoctorales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad Administrativa			
Identificador único*	UA-3		
(Nombre del sistema A1) *	Expediente Físico de Prestadores de Servicios Profesionales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad Administrativa			
Identificador único*	UA-4		
(Nombre del sistema A1) *	Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Secretaría Académica			
Identificador único*	SA-1		
(Nombre del sistema A1) *	Sistema para la Administración de Asuntos Académico-Administrativos		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Secretaría Académica			
Identificador único*	SA-2		
(Nombre del sistema A1) *	Sistema de Información Académica		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualizar a versiones recientes las bibliotecas sobre las que está desarrollado el sistema	*Mantener en sus últimas versiones las dependencias de software sobre las que se encuentra funcionando el sistema*	*Realización contínua*	*Completa*

Coordinación Administrativa del Posgrado de Matemáticas			
Identificador único*	PCCM-1		
(Nombre del sistema A1) *	Sistema de ingreso para alumnos de posgrado		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Coordinación Administrativa del Posgrado de Matemáticas

Identificador único*	PCCM-2		
(Nombre del sistema A1) *	Sistema Integral de Administración Escolar del Posgrado		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad de Documentación - Biblioteca			
Identificador único*	UDB-1		
(Nombre del sistema A1) *	Sistema Integral de Automatización de Bibliotecas Koha		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

La DGBSDI se encarga del resguardo, cuidado y mantenimiento de la información de este sistema.

Unidad de Documentación - Biblioteca			
Identificador único*	UDB-2		
(Nombre del sistema A1) *	Formato de Registro de Usuarios de la Biblioteca		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantener bajo llave este formato en el archivero ubicado en las oficinas de la Biblioteca	*El acceso a este Formato de Registro de Usuarios de la Biblioteca solo se da al personal autorizado.*	*Semestral*	*Dependerá de la vigencia del tipo de usuario*

Unidad de Docencia			
Identificador único*	UDC-1		
(Nombre del sistema A1) *	Sistema de Registro para Participación en Eventos del CCM		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualizar a versiones recientes las bibliotecas sobre las que está desarrollado el sistema	*Mantener en sus últimas versiones las dependencias de software sobre las que se encuentra funcionando el sistema*	*Realización contínua*	*Completa*

Dirección			
Identificador único*	DIR-1		
(Nombre del sistema A1) *	Formato de Seguros		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIA DE DATOS PERSONALES

Bienes y Suministros	
Identificador único*	**ByS**
(Nombre del sistema A1)*	**Sistema Institucional de Compras**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	*No se realizan transferencias de datos personales mediante soportes físicos.*
Transferencias mediante el traslado de soportes electrónicos:	*No se realizan transferencias de datos personales mediante soportes electrónicos.*
Transferencias mediante el traslado sobre redes electrónicas:	*No se realizan transferencias de datos personales sobre redes electrónicas.*

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

Los expedientes físicos se archivan en carpetas y se resguardan bajo llave en mobiliario institucional.

Se cuenta con mobiliario institucional protegido con cerraduras y oficinas con cerraduras en sus puertas.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Nombre: *Adriana Briseño Chávez*
Cargo: *Delegada Administrativa*
Funciones: *Planear, organizar, dirigir, coordinar actividades de apoyo administrativo. Formular programas de trabajo, vigilar recursos asignados, tomar decisiones referente al control y registro de personal, integrar, resguardar y manejar la información y documentación confidencial. Conservar y consolidar la comunicación con la Dirección General de Servicios Generales en lo relativo al programa de Protección Civil. Apoyar al personal académico en aspectos administrativos que requieran. Auxiliar al Director en la elaboración del anteproyecto de presupuesto, entre otras.*

Obligaciones: *Administración de los recursos humanos, presupuestales, materiales y de servicios que se brindan a las áreas de la entidad. Control, supervisión y seguimiento del personal, presupuesto, bienes, suministro, mantenimiento y conservación, así como de aspectos relacionados con las atribuciones en materia de administración. Controlar y vigilar los recursos asignados a los programas institucionales y externos en que participe la entidad. Organizar los asuntos administrativos y cualquier otro que mejore la eficiencia de los procesos de trabajo de las áreas que integran la Delegación Administrativa. Fiscalización del fondo fijo así como vigilar su adecuada aplicación y comprobación. Recopilación, integración, análisis y presentación de informes, docmentos y cualquier elemento solicitado por los órganos de auditoria, fiscalización y control interno. Guardar reserva y/o confidencialidad de todos los asuntos que sean encomendados. Generar y presentar los reportes e informes que sean solicitados por el Director de la Dependencia. Vigilar el cumplimiento de las normas y procedimientos, así como aplicar las políticas de la entidad. Realizar actividades de inspección, vigilancia y fiscalización, así como todos los trabajos personales y confidenciales que por necesidades de la Institución se le requieran y aquellas inherentes a su puesto que sean encomendadas por el Director de la Dependencia.*

Nombre: *Hermelidia Santibáñez Núñez*
Cargo: *Responsable de Bienes y Suministros*
Funciones: *Registro, verificación y control de las compras de bienes y suministros.*
Obligaciones: *Administración, registro, supervisión y control de los bienes y suministros adquiridos.*

III. 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;
   b) Para soportes físicos: Número o clave del expediente utilizado, y
   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
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
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

   Actualmente no se cuenta con bitácoras.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) La metodología aplicada;
   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.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y

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

En caso de suscitarse algún evento se solicita el apoyo del área jurídica de la Coordinación de Servicios Administrativos UNAM Campus Morelia. Para el caso de los soportes electrónicos nosotros no somos responsables de administrar el servidor y sus servicios.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No son identificadas

b) ¿Cómo las autentifica?
No son autentificadas

c) ¿Cómo les autoriza el acceso?
El acceso es libre

La Coordinación de Servicios Administrativos del Campus Morelia de la UNAM es la responsable de la seguridad y vigilancia las 24 horas.

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   No se identifican
2. ¿Cómo las autentifica?
   No se autentifican
3. ¿Cómo les autoriza el acceso?
   El acceso es restringido a las oficinas y sus estantes.

Los soportes físicos se encuentran dentro de la oficina con cerradura. A la persona responsable se le han asignado llaves para abrir puertas y estantería.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

No se cuenta con un mecanismo o procedimiento institucional para la actualización de la información personal.

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

VII. 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.

El Sistema Institucional de Compras es una aplicación vía WEB elaborada por la Secretaria Administrativa de la UNAM y administrado por la Dirección General de Proveeduría por lo que no se tiene acceso a toda la información.

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

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

No aplica

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

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
No
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?

No aplica

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

No aplica

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
b) ¿Quién autoriza la creación de nuevos perfiles?
c) ¿Se lleva registro de la creación de nuevos perfiles?

No aplica

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?

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

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

No aplica

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   - **a)** Completos__, diferenciales ___ o incrementales___;
   - **b)** De forma automática ____ o Manual _____,
   - **c)** Periodicidad con que los realiza: _____

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

3. Cómo y dónde archiva esos medios, y

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

No aplica

IX. 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.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

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.

Actualmente no se cuenta con un plan de contingencia.

I. TRANSFERENCIA DE DATOS PERSONALES

Unidad Administrativa	
Identificador único*	**UA-1**
(Nombre del sistema A1)*	**Sistema Integral de Personal. Expediente Físico**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	*No se realizan transferencias de datos personales mediante soportes físicos.*

Transferencias mediante el traslado de soportes electrónicos:	*No se realizan transferencias de datos personales mediante soportes electrónicos.*
Transferencias mediante el traslado sobre redes electrónicas:	*No se realizan transferencias de datos personales sobre redes electrónicas.*

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

Los soportes físicos se resguardan dentro de una oficina con cerradura, en un archivero con cerradura perteneciente al mobiliario institucional

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Nombre: *Adriana Briseño Chávez*
Cargo: *Delegada Administrativa*
Funciones: *Planear, organizar, dirigir, coordinar actividades de apoyo administrativo. Formular programas de trabajo, vigilar recursos asignados, tomar decisiones referente al control y registro de personal, integrar, resguardar y manejar la información y documentación confidencial. Conservar y consolidar la comunicación con la Dirección General de Servicios Generales en lo relativo al programa de Protección Civil. Apoyar al personal académico en aspectos administrativos que requieran. Auxiliar al Director en la elaboración del anteproyecto de presupuesto, entre otras.*
Obligaciones: Administración de los recursos humanos, presupuestales, materiales y de servicios que se brindan a las áreas de la entidad. Control, supervisión y seguimiento del personal, presupuesto, bienes, suministro, mantenimiento y conservación, así como de aspectos relacionados con las atribuciones en materia de administración. Controlar y vigilar los recursos asignados a los programas institucionales y externos en que participe la entidad. Organizar los asuntos administrativos y cualquier otro que mejore la eficiencia de los procesos de trabajo de las áreas que integran la Delegación Administrativa. Fiscalización del fondo fijo así como vigilar su adecuada aplicación y comprobación. Recopilación, integración, análisis y presentación de informes, docmentos y cualquier elemento solicitado por los órganos de auditoria, fiscalización y control interno. Guardar reserva y/o confidencialidad de todos los asuntos que sean encomendados. Generar y presentar los reportes e informes que sean solicitados por el Director de la Dependencia. Vigilar el cumplimiento de las normas y procedimientos, así como aplicar las políticas de la entidad. Realizar actividades de inspección, vigilancia y fiscalización, así como todos los trabajos personales y confidenciales que por necesidades de la Institución se le requieran y aquellas inherentes a su puesto que sean encomendadas por el Director de la Dependencia.

III. 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;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
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
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

No se cuenta con bitácoras porque no se brinda el servicio de consulta de información.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

En caso de suscitarse algún evento se solicita el apoyo del área jurídica de la Coordinación de Servicios Administrativos UNAM Campus Morelia.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No son identificadas
b) ¿Cómo las autentifica?
No son autentificadas
c) ¿Cómo les autoriza el acceso?
El acceso es libre

La Coordinación de Servicios Administrativos del Campus Morelia de la UNAM es la responsable de la seguridad y vigilancia las 24 horas.

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Los soportes físicos se encuentran dentro de la oficina con cerradura perteneciente a la responsable a quien se le han asignado llaves para abrir puertas y estantería.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   No se identifican
2. ¿Cómo las autentifica?
   No se autentifican
3. ¿Cómo les autoriza el acceso?
   El acceso es restringido a las oficinas y sus estantes.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

No se cuenta con un mecanismo o procedimiento institucional para la actualización de la información personal.

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

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

No aplica

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

No aplica

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?
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

No aplica

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles?

b) ¿Quién autoriza la creación de nuevos perfiles?
c) ¿Se lleva registro de la creación de nuevos perfiles?

No aplica

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?
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
c) ¿Cómo se evita el acceso remoto no autorizado?

No aplica

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

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

No aplica

IX. 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.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
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.

Actualmente no se cuenta con un plan de contingencia.

I. TRANSFERENCIA DE DATOS PERSONALES

Unidad Administrativa	
Identificador único*	**UA-2**
(Nombre del sistema A1)*	**Expediente Físico Becarios Posdoctorales**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	*No se realizan transferencias de datos personales mediante soportes físicos.*

Transferencias mediante el traslado de soportes electrónicos:	*No se realizan transferencias de datos personales mediante soportes electrónicos.*
Transferencias mediante el traslado sobre redes electrónicas:	*No se realizan transferencias de datos personales sobre redes electrónicas.*

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

Los soportes físicos se resguardan dentro de una oficina con cerradura, en un archivero con cerradura perteneciente al mobiliario institucional.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Nombre: *Adriana Briseño Chávez*
Cargo: *Delegada Administrativa*
Funciones: *Planear, organizar, dirigir, coordinar actividades de apoyo administrativo. Formular programas de trabajo, vigilar recursos asignados, tomar decisiones referente al control y registro de personal, integrar, resguardar y manejar la información y documentación confidencial. Conservar y consolidar la comunicación con la Dirección General de Servicios Generales en lo relativo al programa de Protección Civil. Apoyar al personal académico en aspectos administrativos que requieran. Auxiliar al Director en la elaboración del anteproyecto de presupuesto, entre otras.*
Obligaciones: Administración de los recursos humanos, presupuestales, materiales y de servicios que se brindan a las áreas de la entidad. Control, supervisión y seguimiento del personal, presupuesto, bienes, suministro, mantenimiento y conservación, así como de aspectos relacionados con las atribuciones en materia de administración. Controlar y vigilar los recursos asignados a los programas institucionales y externos en que participe la entidad. Organizar los asuntos administrativos y cualquier otro que mejore la eficiencia de los procesos de trabajo de las áreas que integran la Delegación Administrativa. Fiscalización del fondo fijo así como vigilar su adecuada aplicación y comprobación. Recopilación, integración, análisis y presentación de informes, docmentos y cualquier elemento solicitado por los órganos de auditoria, fiscalización y control interno. Guardar reserva y/o confidencialidad de todos los asuntos que sean encomendados. Generar y presentar los reportes e informes que sean solicitados por el Director de la Dependencia. Vigilar el cumplimiento de las normas y procedimientos, así como aplicar las políticas de la entidad. Realizar actividades de inspección, vigilancia y fiscalización, así como todos los trabajos personales y confidenciales que por necesidades de la Institución se le requieran y aquellas inherentes a su puesto que sean encomendadas por el Director de la Dependencia.

III. 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;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la

base de datos.

2. Si las bitácoras están en soporte físico o en soporte electrónico;

3. Lugar dónde almacena las bitácoras y por cuánto tiempo;

4. La manera en que asegura la integridad de las bitácoras, y

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

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

No se cuenta con bitácoras porque no se brinda el servicio de consulta de información.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:

a) La persona que resolvió el incidente;

b) La metodología aplicada;

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.

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

3. Cómo asegura la integridad de dicho registro, y

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

En caso de suscitarse algún evento se solicita el apoyo del área jurídica de la Coordinación de Servicios Administrativos UNAM Campus Morelia.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?

No son identificadas

b) ¿Cómo las autentifica?

No son autentificadas

c) ¿Cómo les autoriza el acceso?

El acceso es libre

La Coordinación de Servicios Administrativos del Campus Morelia de la UNAM es la responsable de la seguridad y vigilancia las 24 horas.

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Los soportes físicos se encuentran dentro de la oficina con cerradura perteneciente a la responsable a quien se le han asignado llaves para abrir puertas y estantería.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   No se identifican
2. ¿Cómo las autentifica?
   No se autentifican
3. ¿Cómo les autoriza el acceso?
   El acceso es restringido a las oficinas y sus estantes.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

No se cuenta con un mecanismo o procedimiento institucional para la actualización de la información personal.

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

VII. 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):

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

No aplica

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

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

No aplica

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?

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

No aplica

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?

b) ¿Quién autoriza la creación de nuevos perfiles?

c) ¿Se lleva registro de la creación de nuevos perfiles?

No aplica

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?

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

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

No aplica

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos__, diferenciales ___ o incrementales___;

b) De forma automática ____ o Manual _____,

c) Periodicidad con que los realiza: _____

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

3. Cómo y dónde archiva esos medios, y

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

No aplica

IX. 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.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

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.

Actualmente no se cuenta con un plan de contingencia.

I. TRANSFERENCIA DE DATOS PERSONALES

Unidad Administrativa	
Identificador único*	**UA-2**
(Nombre del sistema A1)*	**Expediente Físico de Prestadores de Servicios Profesionales**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	*No se realizan transferencias de datos personales mediante soportes físicos.*
Transferencias mediante el traslado de soportes electrónicos:	*No se realizan transferencias de datos personales mediante soportes electrónicos.*
Transferencias mediante el traslado sobre redes electrónicas:	*No se realizan transferencias de datos personales sobre redes electrónicas.*

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

Los soportes físicos se resguardan dentro de una oficina con cerradura, en un archivero con cerradura perteneciente al mobiliario institucional.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Nombre: *Adriana Briseño Chávez*
Cargo: *Delegada Administrativa*
Funciones: *Planear, organizar, dirigir, coordinar actividades de apoyo administrativo. Formular programas de trabajo, vigilar recursos asignados, tomar decisiones referente al control y registro de personal, integrar, resguardar y manejar la información y documentación confidencial. Conservar y consolidar la comunicación con la Dirección General de Servicios Generales en lo relativo al programa de Protección Civil. Apoyar al personal académico en aspectos administrativos que requieran. Auxiliar al Director en la elaboración del anteproyecto de presupuesto, entre otras.*
Obligaciones: Administración de los recursos humanos, presupuestales, materiales y de servicios que se

brindan a las áreas de la entidad. Control, supervisión y seguimiento del personal, presupuesto, bienes, suministro, mantenimiento y conservación, así como de aspectos relacionados con las atribuciones en materia de administración. Controlar y vigilar los recursos asignados a los programas institucionales y externos en que participe la entidad. Organizar los asuntos administrativos y cualquier otro que mejore la eficiencia de los procesos de trabajo de las áreas que integran la Delegación Administrativa. Fiscalización del fondo fijo así como vigilar su adecuada aplicación y comprobación. Recopilación, integración, análisis y presentación de informes, docmentos y cualquier elemento solicitado por los órganos de auditoria, fiscalización y control interno. Guardar reserva y/o confidencialidad de todos los asuntos que sean encomendados. Generar y presentar los reportes e informes que sean solicitados por el Director de la Dependencia. Vigilar el cumplimiento de las normas y procedimientos, así como aplicar las políticas de la entidad. Realizar actividades de inspección, vigilancia y fiscalización, así como todos los trabajos personales y confidenciales que por necesidades de la Institución se le requieran y aquellas inherentes a su puesto que sean encomendadas por el Director de la Dependencia.

III. 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;

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

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

2. Si las bitácoras están en soporte físico o en soporte electrónico;

3. Lugar dónde almacena las bitácoras y por cuánto tiempo;

4. La manera en que asegura la integridad de las bitácoras, y

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

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

No se cuenta con bitácoras porque no se brinda el servicio de consulta de información.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

2. Los datos que registra:

a) La persona que resolvió el incidente;

b) La metodología aplicada;

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.

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

4. Cómo asegura la integridad de dicho registro, y

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

En caso de suscitarse algún evento se solicita el apoyo del área jurídica de la Coordinación de Servicios Administrativos UNAM Campus Morelia.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No son identificadas
b) ¿Cómo las autentifica?
No son autentificadas
c) ¿Cómo les autoriza el acceso?
El acceso es libre

La Coordinación de Servicios Administrativos del Campus Morelia de la UNAM es la responsable de la seguridad y vigilancia las 24 horas.

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Los soportes físicos se encuentran dentro de la oficina con cerradura perteneciente a la responsable a quien se le han asignado llaves para abrir puertas y estantería.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   No se identifican
2. ¿Cómo las autentifica?
   No se autentifican
3. ¿Cómo les autoriza el acceso?
   El acceso es restringido a las oficinas y sus estantes.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

No se cuenta con un mecanismo o procedimiento institucional para la actualización de la información personal.

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

VII. 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):

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

No aplica

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

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

No aplica

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

No aplica

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
b) ¿Quién autoriza la creación de nuevos perfiles?
c) ¿Se lleva registro de la creación de nuevos perfiles?

No aplica

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?
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
c) ¿Cómo se evita el acceso remoto no autorizado?

No aplica

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos__, diferenciales ___ o incrementales___;

b) De forma automática ____ o Manual _____,

c) Periodicidad con que los realiza: _____

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

3. Cómo y dónde archiva esos medios, y

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

No aplica

IX. 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.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

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.

Actualmente no se cuenta con un plan de contingencia.

I. TRANSFERENCIA DE DATOS PERSONALES

Unidad Administrativa	
Identificador único*	**UA-3**
(Nombre del sistema A1)*	**Expediente Físico de Prestadores de Servicios Profesionales**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	*No se realizan transferencias de datos personales mediante soportes físicos.*
Transferencias mediante el traslado de soportes electrónicos:	*No se realizan transferencias de datos personales mediante soportes electrónicos.*
Transferencias mediante el traslado sobre redes electrónicas:	*No se realizan transferencias de datos personales sobre redes electrónicas.*

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

Los soportes físicos se resguardan dentro de una oficina con cerradura, en un archivero con cerradura perteneciente al mobiliario institucional.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Nombre: *Adriana Briseño Chávez*
Cargo: *Delegada Administrativa*
Funciones: *Planear, organizar, dirigir, coordinar actividades de apoyo administrativo. Formular programas de trabajo, vigilar recursos asignados, tomar decisiones referente al control y registro de personal, integrar, resguardar y manejar la información y documentación confidencial. Conservar y consolidar la comunicación con la Dirección General de Servicios Generales en lo relativo al programa de Protección Civil. Apoyar al personal académico en aspectos administrativos que requieran. Auxiliar al Director en la elaboración del anteproyecto de presupuesto, entre otras.*
Obligaciones: Administración de los recursos humanos, presupuestales, materiales y de servicios que se brindan a las áreas de la entidad. Control, supervisión y seguimiento del personal, presupuesto, bienes, suministro, mantenimiento y conservación, así como de aspectos relacionados con las atribuciones en materia de administración. Controlar y vigilar los recursos asignados a los programas institucionales y externos en que participe la entidad. Organizar los asuntos administrativos y cualquier otro que mejore la eficiencia de los procesos de trabajo de las áreas que integran la Delegación Administrativa. Fiscalización del fondo fijo así como vigilar su adecuada aplicación y comprobación. Recopilación, integración, análisis y presentación de informes, docmentos y cualquier elemento solicitado por los órganos de auditoria, fiscalización y control interno. Guardar reserva y/o confidencialidad de todos los asuntos que sean encomendados. Generar y presentar los reportes e informes que sean solicitados por el Director de la Dependencia. Vigilar el cumplimiento de las normas y procedimientos, así como aplicar las políticas de la entidad. Realizar actividades de inspección, vigilancia y fiscalización, así como todos los trabajos personales y confidenciales que por necesidades de la Institución se le requieran y aquellas inherentes a su puesto que sean encomendadas por el Director de la Dependencia.

III. 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;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
5. Respecto del análisis de las bitácoras:
c) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
d) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

No se cuenta con bitácoras porque no se brinda el servicio de consulta de información.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
a) La persona que resolvió el incidente;
b) La metodología aplicada;
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.

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

3. Cómo asegura la integridad de dicho registro, y

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

En caso de suscitarse algún evento se solicita el apoyo del área jurídica de la Coordinación de Servicios Administrativos UNAM Campus Morelia.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No son identificadas

b) ¿Cómo las autentifica?
No son autentificadas

c) ¿Cómo les autoriza el acceso?
El acceso es libre

La Coordinación de Servicios Administrativos del Campus Morelia de la UNAM es la responsable de la seguridad y vigilancia las 24 horas.

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Los soportes físicos se encuentran dentro de la oficina con cerradura perteneciente a la responsable a quien se le han asignado llaves para abrir puertas y estantería.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   No se identifican
2. ¿Cómo las autentifica?
   No se autentifican

3. ¿Cómo les autoriza el acceso?
   El acceso es restringido a las oficinas y sus estantes.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

No se cuenta con un mecanismo o procedimiento institucional para la actualización de la información personal.

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

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

No aplica

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

No aplica

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?
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

No aplica

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles?
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?

No aplica

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

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

No aplica

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos__, diferenciales ___ o incrementales___;

b) De forma automática ____ o Manual _____,

c) Periodicidad con que los realiza: _____

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

3. Cómo y dónde archiva esos medios, y

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

No aplica

IX. PLAN DE CONTINGENCIA

4. 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.

5. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

6. 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.

Actualmente no se cuenta con un plan de contingencia.

I. TRANSFERENCIA DE DATOS PERSONALES

Unidad Administrativa	
Identificador único*	**UA-4**
(Nombre del sistema A1)*	**Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	*No se realizan transferencias de datos personales mediante soportes físicos.*
Transferencias mediante el traslado de soportes electrónicos:	*No se realizan transferencias de datos personales mediante soportes electrónicos.*
Transferencias mediante el traslado sobre redes electrónicas:	*No se realizan transferencias de datos personales sobre redes electrónicas.*

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

Los soportes físicos se resguardan dentro de una oficina con cerradura, en un archivero con cerradura perteneciente al mobiliario institucional

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Nombre: *Adriana Briseño Chávez*
Cargo: *Delegada Administrativa*
Funciones: *Planear, organizar, dirigir, coordinar actividades de apoyo administrativo. Formular programas de trabajo, vigilar recursos asignados, tomar decisiones referente al control y registro de personal, integrar, resguardar y manejar la información y documentación confidencial. Conservar y consolidar la comunicación con la Dirección General de Servicios Generales en lo relativo al programa de Protección Civil. Apoyar al personal académico en aspectos administrativos que requieran. Auxiliar al Director en la elaboración del anteproyecto de presupuesto, entre otras.*
Obligaciones: Administración de los recursos humanos, presupuestales, materiales y de servicios que se brindan a las áreas de la entidad. Control, supervisión y seguimiento del personal, presupuesto, bienes, suministro, mantenimiento y conservación, así como de aspectos relacionados con las atribuciones en materia de administración. Controlar y vigilar los recursos asignados a los programas institucionales y externos en que participe la entidad. Organizar los asuntos administrativos y cualquier otro que mejore la eficiencia de los procesos de trabajo de las áreas que integran la Delegación Administrativa. Fiscalización del fondo fijo así como vigilar su adecuada aplicación y comprobación. Recopilación, integración, análisis y presentación de informes, docmentos y cualquier elemento solicitado por los órganos de auditoria, fiscalización y control interno. Guardar reserva y/o confidencialidad de todos los asuntos que sean encomendados. Generar y presentar los reportes e informes que sean solicitados por el Director de la Dependencia. Vigilar el cumplimiento de las normas y procedimientos, así como aplicar las políticas de la entidad. Realizar actividades de inspección, vigilancia y fiscalización, así como todos los trabajos personales y confidenciales que por necesidades de la Institución se le requieran y aquellas inherentes a su puesto que sean encomendadas por el Director de la Dependencia.

III. 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;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
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
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

No se cuenta con bitácoras porque no se brinda el servicio de consulta de información.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
a) La persona que resolvió el incidente;
b) La metodología aplicada;
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.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

En caso de suscitarse algún evento se solicita el apoyo del área jurídica de la Coordinación de Servicios Administrativos UNAM Campus Morelia.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Los soportes físicos se encuentran dentro de la oficina con cerradura perteneciente a la responsable a quien se le han asignado llaves para abrir puertas y estantería.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
No son identificadas
b) ¿Cómo las autentifica?
No son autentificadas
c) ¿Cómo les autoriza el acceso?
El acceso es libre

La Coordinación de Servicios Administrativos del Campus Morelia de la UNAM es la responsable de la seguridad y vigilancia las 24 horas.

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Los soportes físicos se encuentran dentro de la oficina con cerradura perteneciente a la responsable a quien se le han asignado llaves para abrir puertas y estantería.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   No se identifican
2. ¿Cómo las autentifica?
   No se autentifican
3. ¿Cómo les autoriza el acceso?
   El acceso es restringido a las oficinas y sus estantes.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

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

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

No aplica

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

No aplica

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?

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

No aplica

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles?
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?

No aplica

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?
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
- **c)** ¿Cómo se evita el acceso remoto no autorizado?

No aplica

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos__, diferenciales ___ o incrementales___;

b) De forma automática ____ o Manual _____,

c) Periodicidad con que los realiza: _____

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

3. Cómo y dónde archiva esos medios, y

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

No aplica

IX. 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.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

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.

Actualmente no se cuenta con un plan de contingencia.

I. TRANSFERENCIA DE DATOS PERSONALES

Secretaría Académica

Identificador único*	**SA-1**
(Nombre del sistema A1)*	**Sistema para la Administración de Asuntos Académicos-Administrativos**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	*Los envíos de documentación se hacen mediante un sobre o paquete cerrado. Se envía acuse de recibo al remitente.*
Transferencias mediante el traslado de soportes electrónicos:	*Los archivos electrónicos que contienen datos personales se colocan en las plataformas oficiales.* *Datos de actividades, proyectos, producción, etc. Son información que alimenta diversos sistemas de la UNAM.*
Transferencias mediante el traslado sobre redes electrónicas:	*Se utiliza una red pública (internet) local. Sí se cuenta con dispositivos. Se solicita acuse electrónico de recepción de la información.*

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

Mediante Instrumentos de Control y Consulta Archivística

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Nombre: *Valdemar Orozco Cárdenas, José Ferrán Valdez Lorenzo, Luis Abel Castorena Martínez*
Cargo: *Auxiliar de la Secretaría Académica, Secretario Académico, Director*
Funciones:
Obligaciones:

III. 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;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
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
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

La Coordinación de la Investigación Científica es la encargada de la administración del sistema.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
a) La persona que resolvió el incidente;
b) La metodología aplicada;
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.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

La Coordinación de la Investigación Científica es la encargada de la administración del sistema.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
b) ¿Cómo las autentifica?
c) ¿Cómo les autoriza el acceso?

La Coordinación de Servicios Administrativos del Campus Morelia de la UNAM es la responsable de la seguridad y vigilancia las 24 horas.

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Los soportes físicos y electrónicos se encuentran dentro de la oficina con cerradura perteneciente a la responsable a quien se le han asignado llaves para abrir puertas y estantería.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   No se identifican
2. ¿Cómo las autentifica?
   No se autentifican
3. ¿Cómo les autoriza el acceso?
   El acceso es restringido a las oficinas y sus estantes.

La Coordinación de la Investigación Científica es la responsable de la administración del sistema.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

La Coordinación de la Investigación Científica es la responsable de la actualización de información del sistema.

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

VII. 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):

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

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

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
  No
- **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?

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?

4. Administración de perfiles de usuario y contraseñas:

- **a)** ¿Quién da de alta nuevos perfiles?
  Coordinación de la Investigación Científica
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
  Coordinación de la Investigación Científica
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?

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?
La Coordinación de la Investigación Científica es la responsable de la administración del sistema

c) ¿Cómo se evita el acceso remoto no autorizado?
La Coordinación de la Investigación Científica es la responsable de la administración del sistema

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos__, diferenciales ___ o incrementales___;

b) De forma automática ____ o Manual _____,

c) Periodicidad con que los realiza: _____

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

3. Cómo y dónde archiva esos medios, y

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

La Coordinación de la Investigación Científica es la responsable de la administración del sistema

IX. 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.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

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.

La Coordinación de la Investigación Científica es la responsable de la administración del sistema

I. TRANSFERENCIA DE DATOS PERSONALES

Secretaría Académica	
Identificador único*	**SA-2**
(Nombre del sistema A1)*	**Sistema de Información Académica**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	*Los envíos de documentación se hacen mediante un sobre o paquete cerrado. Se envía acuse de recibo al remitente.*

Transferencias mediante el traslado de soportes electrónicos:	*Los archivos electrónicos que contienen datos personales se colocan en las plataformas oficiales.* *Datos de actividades, proyectos, producción, etc. Son información que alimenta diversos sistemas de la UNAM.*
Transferencias mediante el traslado sobre redes electrónicas:	*Se utiliza una red pública (internet) local. Sí se cuenta con dispositivos. Se solicita acuse electrónico de recepción de la información.*

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

Mediante Instrumentos de Control y Consulta Archivística

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Nombre: *Valdemar Orozco Cárdenas, José Ferrán Valdez Lorenzo, Luis Abel Castorena Martínez*
Cargo: *Auxiliar de la Secretaría Académica, Secretario Académico, Director*
Funciones:
Obligaciones:

III. 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;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
5. Respecto del análisis de las bitácoras:
c) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
d) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

Actualmente no se cuenta con bitácoras.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

5. Los datos que registra:
a) La persona que resolvió el incidente;
b) La metodología aplicada;
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.
6. Si el registro está en soporte físico o en soporte electrónico;
7. Cómo asegura la integridad de dicho registro, y
8. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

Actualmente no se cuenta con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
b) ¿Cómo las autentifica?
c) ¿Cómo les autoriza el acceso?

La Coordinación de Servicios Administrativos del Campus Morelia de la UNAM es la responsable de la seguridad y vigilancia las 24 horas.

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Los soportes físicos y electrónicos se encuentran dentro de la oficina con cerradura perteneciente a la responsable a quien se le han asignado llaves para abrir puertas y estantería.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   No se identifican
2. ¿Cómo las autentifica?
   No se autentifican
3. ¿Cómo les autoriza el acceso?
   El acceso es restringido a las oficinas y sus estantes.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

Actualmente no se cuenta con un procedimiento para la actualización de la información.

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

VII. 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):

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

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

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

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?
Sí

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Secretaría Académica
b) ¿Quién autoriza la creación de nuevos perfiles?
Secretaría Académica
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?
Lista de usuarios permitidos para el acceso remoto

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos_X_, diferenciales ___ o incrementales___;

b) De forma automática __X__ o Manual _X___,

c) Periodicidad con que los realiza: __diario____

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
   Equipo dedicado a respaldos
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   Unidad de Cómputo

IX. 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.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
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.

Actualmente no se cuenta con un plan de contingencia.

I. TRANSFERENCIA DE DATOS PERSONALES

Coordinación Administrativa del Posgrado de Matemáticas	
Identificador único*	**PCCM-1**
(Nombre del sistema A1)*	**Sistema de ingreso para alumnos de posgrado**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	*No se realizan transferencias de datos personales mediante soportes físicos.*
Transferencias mediante el traslado de soportes electrónicos:	*No se realizan transferencias de datos personales mediante soportes electrónicos.*
Transferencias mediante el traslado sobre redes electrónicas:	*No se realizan transferencias de datos personales sobre redes electrónicas.*

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

Actualmente la Drección General de Administración Escolar se resguarda toda la documentación original de expedientes de alumnos. De manera interna se resguarda en archiveros y en electrónico (PC).

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Nombre: *Morelia Ibone Alvarez Llanes*
Cargo: *Jefe de Área*
Funciones:

- *Gestionar el proceso de admisión, inscripción, permanencia y obtención de grado de los alumnos*
- *del PCCM.*
- *Controlar los recursos financieros asignados al PCCM.*
- *Elaborar, gestionar y publicar de las convocatorias de ingreso para los alumnos de posgrado de Maestría y Doctorado.*
- *Integrar la documentación para la formación de expedientes de los alumnos al PCCM.*
- *Planear las actividades académicas del personal docente del PCCM.*
- *Integrar la información requerida para oficializar el ingreso de los alumnos a la UNAM.*
- *Gestionar las postulaciones de los alumnos admitidos al PCCM para que se incorporen en el programa de Becas Nacionales CONACyT.*
- *Planear y controlar la asignación de materias a impartir por el personal docente a los alumnos PCCM.*
- *Gestionar la incorporación de los tutores al Sistema de Firma Electrónica Avanzada de la UNAM.*
- *Supervisar que el personal docente evalúe en tiempo forma a los alumnos del PCCM.*
- *Gestionar la postulación de los Becarios Posdoctorales al Programa de Becas Nacionales de Posdoctorales de CONACyT.*
- *Elaborar los documentos para la evaluación de los Programas de Posgrado del PCCM para diferentes entidades, (CONACyT, UNAM, UMSNH, entre otros).*

Obligaciones: *Control, seguimiento de trámites administrativos.*

III. 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;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
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
b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

La Dirección General de Administración Escolar es la encargada de la administración del sistema.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
a) La persona que resolvió el incidente;
b) La metodología aplicada;
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.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

Actualmente no se cuenta con un procedimiento para la atención de incidentes.

La Dirección General de Administración Escolar es la encargada de la administración del sistema.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
b) ¿Cómo las autentifica?
c) ¿Cómo les autoriza el acceso?

La Coordinación de Servicios Administrativos del Campus Morelia de la UNAM es la responsable de la seguridad y vigilancia las 24 horas.

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
2. ¿Cómo las autentifica?
3. ¿Cómo les autoriza el acceso?

Los soportes físicos se encuentran dentro de la oficina con cerradura perteneciente a la responsable a quien se le han asignado llaves para abrir puertas y estantería.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

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

VII. 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):

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

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

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

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

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
b) ¿Quién autoriza la creación de nuevos perfiles?
c) ¿Se lleva registro de la creación de nuevos perfiles?

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?
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
c) ¿Cómo se evita el acceso remoto no autorizado?

La Dirección General de Administración Escolar es la encargada de la administración del sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos__, diferenciales ___ o incrementales___;
b) De forma automática ____ o Manual _____,
c) Periodicidad con que los realiza: _____

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;
3. Cómo y dónde archiva esos medios, y

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

La Dirección General de Administración Escolar es la encargada de la administración del sistema.

IX. 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.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

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.

La Dirección General de Administración Escolar es la encargada de la administración del sistema.

I. TRANSFERENCIA DE DATOS PERSONALES

Coordinación Administrativa del Posgrado de Matemáticas	
Identificador único*	**PCCM-2**
(Nombre del sistema A1)*	**Sistema Integral de Administración Escolar del Posgrado**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	*No se realizan transferencias de datos personales mediante soportes físicos.*
Transferencias mediante el traslado de soportes electrónicos:	*No se realizan transferencias de datos personales mediante soportes electrónicos.*
Transferencias mediante el traslado sobre redes electrónicas:	*No se realizan transferencias de datos personales sobre redes electrónicas.*

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

Actualmente la Drección General de Administración Escolar se resguarda toda la documentación original de expedientes de alumnos. De manera interna se resguarda en archiveros y en electrónico (PC).

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Nombre: *Morelia Ibone Alvarez Llanes*
Cargo: *Jefe de Área*
Funciones:

- *Gestionar el proceso de admisión, inscripción, permanencia y obtención de grado de los alumnos*
- *del PCCM.*
- *Controlar los recursos financieros asignados al PCCM.*
- *Elaborar, gestionar y publicar de las convocatorias de ingreso para los alumnos de posgrado de Maestría y Doctorado.*
- *Integrar la documentación para la formación de expedientes de los alumnos al PCCM.*
- *Planear las actividades académicas del personal docente del PCCM.*
- *Integrar la información requerida para oficializar el ingreso de los alumnos a la UNAM.*
- *Gestionar las postulaciones de los alumnos admitidos al PCCM para que se incorporen en el programa de Becas Nacionales CONACyT.*
- *Planear y controlar la asignación de materias a impartir por el personal docente a los alumnos PCCM.*
- *Gestionar la incorporación de los tutores al Sistema de Firma Electrónica Avanzada de la UNAM.*
- *Supervisar que el personal docente evalúe en tiempo forma a los alumnos del PCCM.*
- *Gestionar la postulación de los Becarios Posdoctorales al Programa de Becas Nacionales de Posdoctorales de CONACyT.*
- *Elaborar los documentos para la evaluación de los Programas de Posgrado del PCCM para diferentes entidades, (CONACyT, UNAM, UMSNH, entre otros).*

Obligaciones: *Control, seguimiento de trámites administrativos.*

III. 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;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
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
  b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

La Dirección General de Administración Escolar es la encargada de la administración del sistema.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

5. Los datos que registra:
a) La persona que resolvió el incidente;
b) La metodología aplicada;
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.

6. Si el registro está en soporte físico o en soporte electrónico;
7. Cómo asegura la integridad de dicho registro, y
8. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

La Dirección General de Administración Escolar es la encargada de la administración del sistema.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
b) ¿Cómo las autentifica?
c) ¿Cómo les autoriza el acceso?

La Coordinación de Servicios Administrativos del Campus Morelia de la UNAM es la responsable de la seguridad y vigilancia las 24 horas.

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Los soportes físicos se encuentran dentro de la oficina con cerradura perteneciente a la responsable a quien se le han asignado llaves para abrir puertas y estantería.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   No se identifican
2. ¿Cómo las autentifica?
   No se autentifican
3. ¿Cómo les autoriza el acceso?
   El acceso es restringido a las oficinas y sus estantes.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

Actualmente no se cuenta con un mecanismo o precedimiento institucional para la actualización de la información.

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

VII. 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):

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

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

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

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

4. Administración de perfiles de usuario y contraseñas:

d) ¿Quién da de alta nuevos perfiles?
a) ¿Quién autoriza la creación de nuevos perfiles?
b) ¿Se lleva registro de la creación de nuevos perfiles?

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?
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
c) ¿Cómo se evita el acceso remoto no autorizado?

La Dirección General de Administración Escolar es la encargada de la administración del sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos__, diferenciales ___ o incrementales___;
b) De forma automática ____ o Manual _____,
c) Periodicidad con que los realiza: _____

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

La Dirección General de Administración Escolar es la encargada de la administración del sistema.

IX. 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.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

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.

La Dirección General de Administración Escolar es la encargada de la administración del sistema.

I. TRANSFERENCIA DE DATOS PERSONALES

Unidad de Documentación - Biblioteca	
Identificador único*	**UDB-1**
(Nombre del sistema A1)*	**Sistema Integral de Automatización de Bibliotecas Koha**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	*No se realizan transferencias de datos personales mediante soportes físicos.*
Transferencias mediante el traslado de soportes electrónicos:	*No se realizan transferencias de datos personales mediante soportes electrónicos.*
Transferencias mediante el traslado sobre redes electrónicas:	*No se realizan transferencias de datos personales sobre redes electrónicas.*

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

La Dirección General de Bibliotecas y Servicios Digitales de Información administra el sistema de gestión Koha.

III. 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;

b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
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
b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

La Dirección General de Bibliotecas y Servicios Digitales de Información administra el sistema de gestión Koha.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

9. Los datos que registra:
a) La persona que resolvió el incidente;
b) La metodología aplicada;
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.
10. Si el registro está en soporte físico o en soporte electrónico;
11. Cómo asegura la integridad de dicho registro, y
12. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

La Dirección General de Bibliotecas y Servicios Digitales de Información administra el sistema de gestión Koha.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
b) ¿Cómo las autentifica?
c) ¿Cómo les autoriza el acceso?

La Coordinación de Servicios Administrativos del Campus Morelia de la UNAM es la responsable de la seguridad y vigilancia las 24 horas.

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
2. ¿Cómo las autentifica?
3. ¿Cómo les autoriza el acceso?

Oficina con cerradura perteneciente a la responsable a quien se le han asignado llaves para abrir puertas y estantería.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

La Dirección General de Bibliotecas y Servicios Digitales de Información administra el sistema de gestión Koha.

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

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

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

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?
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Personal de la DGBSDI
c) ¿Quién autoriza la creación de nuevos perfiles?
Los técnicos académicos de la biblioteca
d) ¿Se lleva registro de la creación de nuevos perfiles?

Sí, se lleva un registro de alta de usuarios y se resguarda en una carpeta físicamente.

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?
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
c) ¿Cómo se evita el acceso remoto no autorizado?

La Dirección General de Bibliotecas y Servicios Digitales de Información administra el sistema de gestión Koha.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

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

La Dirección General de Bibliotecas y Servicios Digitales de Información administra el sistema de gestión Koha.

IX. 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.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
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.

La Dirección General de Bibliotecas y Servicios Digitales de Información administra el sistema de gestión Koha.

I. TRANSFERENCIA DE DATOS PERSONALES

Unidad de Documentación - Biblioteca

Identificador único*	**UDB-2**
(Nombre del sistema A1)*	**Formato de Registro de Usuarios de la Biblioteca**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	*No se realizan transferencias de datos personales mediante soportes físicos.*
Transferencias mediante el traslado de soportes electrónicos:	*No se realizan transferencias de datos personales mediante soportes electrónicos.*
Transferencias mediante el traslado sobre redes electrónicas:	*No se realizan transferencias de datos personales sobre redes electrónicas.*

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

Se resguarda en una carpeta dentro del mobiliario institucional perteneciente a la biblioteca.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Nombre: *Lidia González García*
Cargo: *Técnica Académica*
Funciones: *Responsable de la Biblioteca*
Obligaciones: *Servicios Bibliotecarios de Información*

Nombre: *Alejandro Medina Alanis*
Cargo: *Técnico Académico*
Funciones: *Responsable Hemeroteca*
Obligaciones: *Servicios Bibliotecarios de Información*

III. 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;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
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
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

El acceso a los datos lo controlamos 2 técnicos académicos responsables de la biblioteca, no tiene número de expediente, se organizan por año, por orden alfabético y se guardan en una carpeta.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
a) La persona que resolvió el incidente;
b) La metodología aplicada;
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.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

Actualmente no se cuenta con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
b) ¿Cómo las autentifica?
c) ¿Cómo les autoriza el acceso?

La Coordinación de Servicios Administrativos del Campus Morelia de la UNAM es la responsable de la seguridad y vigilancia las 24 horas.

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
2. ¿Cómo las autentifica?
3. ¿Cómo les autoriza el acceso?

Los soportes físicos se encuentran dentro de la biblioteca con cerraduras, a los responsables se les han asignado llaves para abrir puertas y estantería.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

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

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

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

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?
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles?
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?

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?
- **e)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
- **f)** ¿Cómo se evita el acceso remoto no autorizado?

No aplica

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos__, diferenciales ___ o incrementales___;

b) De forma automática ____ o Manual _____,

c) Periodicidad con que los realiza: _____

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

3. Cómo y dónde archiva esos medios, y

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

No aplica

IX. 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.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

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.

Actualmente no se cuenta con un plan de contingencia.

I. TRANSFERENCIA DE DATOS PERSONALES

Unidad de Docencia	
Identificador único*	**UDC-1**
(Nombre del sistema A1)*	**Sistema de Registro para Participación en Eventos del CCM**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales mediante soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales mediante soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales sobre redes electrónicas.

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

No aplica

III. 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;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
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
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

Actualmente no se tienen bitácoras.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
a) La persona que resolvió el incidente;
b) La metodología aplicada;
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.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

Actualmente no se tiene un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene

vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
b) ¿Cómo las autentifica?
c) ¿Cómo les autoriza el acceso?

La Coordinación de Servicios Administrativos del Campus Morelia de la UNAM es la responsable de la seguridad y vigilancia las 24 horas.

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
2. ¿Cómo las autentifica?
3. ¿Cómo les autoriza el acceso?

El centro de datos cuenta con cerradura solo los responsables de la Unidad deCñomputo cuentan con llaves para abrir puertas.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

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

Actualmente no se cuenta con un mecanismo o procedimiento para la actualización de la información

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

d) ¿Está basado en reglas?

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

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

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

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

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?
Sí

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Unidad de Cómputo

b) ¿Quién autoriza la creación de nuevos perfiles?
Unidad de Docencia

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?
Lista de usuarios permitidos, contraseñas seguras

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

a) Completos_X_, diferenciales ___ o incrementales___;

b) De forma automática __X__ o Manual __X__,

c) Periodicidad con que los realiza: __diario_____

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
Equipo dedicado a respaldos

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
Unidad de Cómputo

IX. 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.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

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.

Actualmente no se cuenta con un plan de contingencia

I. TRANSFERENCIA DE DATOS PERSONALES

Asistente Dirección	
Identificador único*	**DIR-1**
(Nombre del sistema A1)*	**Formato de Seguros**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	*No se realizan transferencias de datos personales mediante soportes físicos.*
Transferencias mediante el traslado de soportes electrónicos:	La comunicación es a través del correo electrónico institucional. La información no es cifrada.
Transferencias mediante el traslado sobre redes electrónicas:	*No se realizan transferencias de datos personales sobre redes electrónicas.*

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

Los soportes físicos se encuentran resguardados en los archivos de la Dirección del Centro y se encuentran en un archivero con llave.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

Nombre: *Jorge Alejandro Romero Rodríguez*
Cargo: *Asistente Ejecutivo de Dirección*
Funciones*: Asistir al Director del Centro en todo lo que se requiera*
Obligaciones*: Resguardar bajo llave los archivos que tienen datos personales para evitar un mal uso de ellos.*

III. 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;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
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
b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
Actualmente no se cuenta con bitácoras.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
a) La persona que resolvió el incidente;
b) La metodología aplicada;
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.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

Actualmente no se cuenta con un procedimiento de atención de incidentes.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
b) ¿Cómo las autentifica?
c) ¿Cómo les autoriza el acceso?

La Coordinación de Servicios Administrativos del Campus Morelia de la UNAM es la responsable de la seguridad y vigilancia las 24 horas.

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
2. ¿Cómo las autentifica?
3. ¿Cómo les autoriza el acceso?

Los soportes físicos se encuentran dentro de la oficina con cerradura perteneciente a la responsable a quien se le han asignado llaves para abrir puertas y estantería.

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

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

Actualmente no se cuenta con un mecanismo o procedimiento institucional para la actualización de la información.

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

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

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?
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?

b) ¿Quién autoriza la creación de nuevos perfiles?

c) ¿Se lleva registro de la creación de nuevos perfiles?

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?

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

c) ¿Cómo se evita el acceso remoto no autorizado?
No aplica

VIII. 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: _____

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

3. Cómo y dónde archiva esos medios, y
Mobiliario institucional con cerradura dentro del lugar del asistente de la Dirección

4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
El área universitaria

IX. 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.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

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.

Actualmente no se cuenta con un plan de contingencia.

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

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

Bienes y Suministros		
Identificador único*	ByS	
(Nombre del sistema A1)*	Sistema Institucional de Compras	
Recurso*	**Descripción***	**Control***
No aplica	*No aplica*	*El sistema es administrado por la Dirección General de Proveeduría*

Unidad Administrativa		
Identificador único*	UA-1	
(Nombre del sistema A1)*	Sistema Integral de Personal. Expediente Físico	
Recurso*	**Descripción***	**Control***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa	
Identificador único*	UA-2
(Nombre del sistema A1)*	Expediente Físico Becarios Posdoctorales

Recurso*	Descripción*	Control*
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-3	
(Nombre del sistema A1)*	Expediente Físico de Prestadores de Servicios Profesionales	
Recurso*	**Descripción***	**Control***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-4	
(Nombre del sistema A1)*	Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT	
Recurso*	**Descripción***	**Control***
No aplica	*No aplica*	*No aplica*

Secretaría Académica		
Identificador único*	SA-1	
(Nombre del sistema A1)*	Sistema para la Administración de Asuntos Académicos-Administrativos	
Recurso*	**Descripción***	**Control***

No aplica	*No aplica*	*El sistema es administrado por la Coordinación de la Investigación Científica*

Secretaría Académica		
Identificador único*	SA-2	
(Nombre del sistema A1)*	Sistema de Información Académica	
Recurso*	**Descripción***	**Control***
No aplica	*No aplica*	*Unidad de Cómputo*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-1	
(Nombre del sistema A1)*	Sistema de ingreso para alumnos de posgrado	
Recurso*	**Descripción***	**Control***
No aplica	*No aplica*	*El sistema es administrado por la Dirección General de Administración Escolar*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-2	
(Nombre del sistema A1)*	Sistema Integral de Administración Escolar del Posgrado	
Recurso*	**Descripción***	**Control***

No aplica	*No aplica*	*El sistema es administrado por la Dirección General de Administración Escolar*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-1	
(Nombre del sistema A1)*	Sistema Integral de Automatización de Bibliotecas Koha	
Recurso*	**Descripción***	**Control***
No aplica	*No aplica*	*El sistema es administrado por la Dirección General de Bibliotecas y Servicios Digitales de Información*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-2	
(Nombre del sistema A1)*	Formato de Registro de Usuarios de la Biblioteca	
Recurso*	**Descripción***	**Control***
No aplica	*No aplica*	*No aplica*

Unidad de Docencia		
Identificador único*	UDC-1	
(Nombre del sistema A1)*	Sistema de Registro para Participación en Eventos del CCM	
Recurso*	**Descripción***	**Control***

No aplica	*No aplica*	*Unidad de Cómputo*

Dirección		
Identificador único*	DIR-1	
(Nombre del sistema A1)*	Formato de Seguros	
Recurso*	**Descripción***	**Control***
No aplica	*No aplica*	*No aplica*

7.2 Procedimiento para la revisión de las medidas de seguridad

Bienes y Suministros		
Identificador único*	ByS	
(Nombre del sistema A1)*	**Sistema Institucional de Compras**	
Medida de seguridad*	**Procedimiento***	**Responsable***
No aplica	*No aplica*	*El sistema es administrado por la Dirección General de Proveeduría*

Unidad Administrativa		
Identificador único*	UA-1	
(Nombre del sistema A1)*	**Sistema Integral de Personal. Expediente Físico**	
Medida de seguridad*	**Procedimiento***	**Responsable***

No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-2	
(Nombre del sistema A1)*	**Expediente Físico Becarios Posdoctorales**	
Medida de seguridad*	**Procedimiento***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-3	
(Nombre del sistema A1)*	**Expediente Físico de Prestadores de Servicios Profesionales**	
Medida de seguridad*	**Procedimiento***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-4	
(Nombre del sistema A1)*	**Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT**	
Medida de seguridad*	**Procedimiento***	**Responsable***
No aplica	*No aplica*	*No aplica*

Secretaría Académica		
Identificador único*	SA-1	
(Nombre del sistema A1)*	**Sistema para la Administración de Asuntos Académicos-Administrativos**	
Medida de seguridad*	**Procedimiento***	**Responsable***
No aplica	*No aplica*	*El sistema es administrado por la Coordinación de la Investigación científica*

Secretaría Académica		
Identificador único*	SA-2	
(Nombre del sistema A1)*	**Sistema de Información Académica**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Respaldo del sistema y su base de datos	*Realización del respaldo del código fuente del sistema, así como de la información contenida en la base de datos*	*Luis Gerardo Tejero Gómez (1 día)*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-1	
(Nombre del sistema A1)*	**Sistema de ingreso para alumnos de posgrado**	
Medida de seguridad*	**Procedimiento***	**Responsable***

No aplica	*No aplica*	*El sistema es administrado por la Dirección General de Administración Escolar*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-2	
(Nombre del sistema A1)*	**Sistema Integral de Administración Escolar del Posgrado**	
Medida de seguridad*	**Procedimiento***	**Responsable***
No aplica	*No aplica*	*El sistema es administrado por la Dirección General de Administración Escolar*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-1	
(Nombre del sistema A1)*	**Sistema Integral de Automatización de Bibliotecas Koha**	
Medida de seguridad*	**Procedimiento***	**Responsable***
No aplica	*No aplica*	*El sistema es administrado por la Dirección General de Bibliotecas y Servicios Digitales de Información*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-2	
(Nombre del sistema A1)*	**Formato de Registro de Usuarios de la Biblioteca**	
Medida de seguridad*	**Procedimiento***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad de Docencia		
Identificador único*	UDC-1	
(Nombre del sistema A1)*	**Sistema de Registro para Participación en Eventos del CCM**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Respaldo del sistema y su base de datos	*Realización del respaldo del código fuente del sistema, así como de la información contenida en la base de datos*	*Luis Gerardo Tejero Gómez (1 día)*

Dirección		
Identificador único*	DIR-1	
(Nombre del sistema A1)*	**Formato de Seguros**	
Medida de seguridad*	**Procedimiento***	**Responsable***
No aplica	*No aplica*	*No aplica*

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

Bienes y Suministros		
Identificador único*	ByS	
(Nombre del sistema A1)*	**Sistema Institucional de Compras**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-1	
(Nombre del sistema A1)*	**Sistema Integral de Personal. Expediente Físico**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-2	
(Nombre del sistema A1)*	**Expediente Físico Becarios Posdoctorales**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-3	
(Nombre del sistema A1)*	**Expediente Físico de Prestadores de Servicios Profesionales**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-4	
(Nombre del sistema A1)*	**Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No aplica	*No aplica*	*No aplica*

Secretaría Académica		
Identificador único*	SA-1	
(Nombre del sistema A1)*	**Sistema para la Administración de Asuntos Académicos-Administrativos**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No aplica	*No aplica*	*No aplica*

Secretaría Académica		
Identificador único*	SA-2	
(Nombre del sistema A1)*	**Sistema de Información Académica**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Respaldo del sistema y de su base de datos	*Se cuenta con el código fuente de la aplicación en un repositorio externo y con respaldos de la base de datos.*	*Luis Gerardo Tejero Gómez*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-1	
(Nombre del sistema A1)*	**Sistema de ingreso para alumnos de posgrado**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No aplica	*No aplica*	*No aplica*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-2	
(Nombre del sistema A1)*	**Sistema Integral de Administración Escolar del Posgrado**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-1	
(Nombre del sistema A1)*	**Sistema Integral de Automatización de Bibliotecas Koha**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-2	
(Nombre del sistema A1)*	**Formato de Registro de Usuarios de la Biblioteca**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad de Docencia		
Identificador único*	UDC-1	
(Nombre del sistema A1)*	**Sistema de Registro para Participación en Eventos del CCM**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Respaldo del sistema y de su base de datos	*Se cuenta con el código fuente de la aplicación en un repositorio externo y con respaldos de la base de datos.*	*Luis Gerardo Tejero Gómez*

Dirección		
Identificador único*	DIR-1	
(Nombre del sistema A1)*	**Formato de Seguros**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
No aplica	*No aplica*	*No aplica*

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

Bienes y Suministros		
Identificador único*	ByS	
(Nombre del sistema A1)*	**Sistema Institucional de Compras**	
Medida de seguridad*	**Acciones***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-1	
(Nombre del sistema A1)*	**Sistema Integral de Personal. Expediente Físico**	
Medida de seguridad*	**Acciones***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-2	
(Nombre del sistema A1)*	**Expediente Físico Becarios Posdoctorales**	
Medida de seguridad*	**Acciones***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-3	
(Nombre del sistema A1)*	**Expediente Físico de Prestadores de Servicios Profesionales**	
Medida de seguridad*	**Acciones***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-4	
(Nombre del sistema A1)*	**Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT**	
Medida de seguridad*	**Acciones***	**Responsable***
No aplica	*No aplica*	*No aplica*

Secretaría Académica		
Identificador único*	SA-1	
(Nombre del sistema A1)*	**Sistema para la Administración de Asuntos Académicos-Administrativos**	
Medida de seguridad*	**Acciones***	**Responsable***
No aplica	*No aplica*	*No aplica*

Secretaría Académica		
Identificador único*	SA-2	
(Nombre del sistema A1)*	**Sistema de Información Académica**	
Medida de seguridad*	**Acciones***	**Responsable***
Mantener actualizado el sistema en las últimas versiones de seguridad que sean posibles	*Aplicar las actualizaciones de seguridad disponibles del lenguaje de programación y el sistema operativo*	*Luis Gerardo Tejero Gómez*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-1	
(Nombre del sistema A1)*	**Sistema de ingreso para alumnos de posgrado**	
Medida de seguridad*	**Acciones***	**Responsable***
No aplica	*No aplica*	*No aplica*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-2	
(Nombre del sistema A1)*	**Sistema Integral de Administración Escolar del Posgrado**	
Medida de seguridad*	**Acciones***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-1	
(Nombre del sistema A1)*	**Sistema Integral de Automatización de Bibliotecas Koha**	
Medida de seguridad*	**Acciones***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-2	
(Nombre del sistema A1)*	**Formato de Registro de Usuarios de la Biblioteca**	
Medida de seguridad*	**Acciones***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad de Docencia		
Identificador único*	UDC-1	
(Nombre del sistema A1)*	**Sistema de Registro para Participación en Eventos del CCM**	
Medida de seguridad*	**Acciones***	**Responsable***
Mantener actualizado el sistema en las últimas versiones de seguridad que sean posibles	*Aplicar las actualizaciones de seguridad disponibles del lenguaje de programación y el sistema operativo*	*Luis Gerardo Tejero Gómez*

Asistente Dirección		
Identificador único*	DIR-1	
(Nombre del sistema A1)*	**Formato de Seguros**	
Medida de seguridad*	**Acciones***	**Responsable***
No aplica	*No aplica*	*No aplica*

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Bienes y Suministros			
Identificador único*	ByS		
(Nombre del sistema A1)*	**Sistema Institucional de Compras**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de capacitación

Unidad Administrativa			
Identificador único*	UA-1		
(Nombre del sistema A1)*	**Sistema Integral de Personal. Expediente Físico**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material	*Describa el tipo de elemento, sus*	*Indique duración del elemento en horas,*	*Mencione público objetivo, vigencia del elemento y*

didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*objetivos y forma de impartición, publicación o distribución*	*días, meses, su fecha de inicio y de término*	*frecuencia de actualización*

Actualmente no se cuenta con un programa de capacitación

Unidad Administrativa			
Identificador único*	UA-2		
(Nombre del sistema A1)*	**Expediente Físico Becarios Posdoctorales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de capacitación

Unidad Administrativa			
Identificador único*	UA-3		
(Nombre del sistema A1)*	**Expediente Físico de Prestadores de Servicios Profesionales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de capacitación

Unidad Administrativa			
Identificador único*	UA-4		
(Nombre del sistema A1)*	**Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de capacitación

Secretaría Académica			
Identificador único*	SA-1		
(Nombre del sistema A1)*	**Sistema para la Administración de Asuntos Académicos-Administrativos**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de capacitación

Secretaría Académica			
Identificador único*	SA-2		
(Nombre del sistema A1)*	**Sistema de Información Académica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de capacitación

Coordinación Administrativa del Posgrado de Matemáticas			
Identificador único*	PCCM-1		
(Nombre del sistema A1)*	**Sistema de ingreso para alumnos de posgrado**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de capacitación

Coordinación Administrativa del Posgrado de Matemáticas			
Identificador único*	PCCM-2		
(Nombre del sistema A1)*	**Sistema Integral de Administración Escolar del Posgrado**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de capacitación

Unidad de Documentación - Biblioteca			
Identificador único*	UDB-1		
(Nombre del sistema A1)*	**Sistema Integral de Automatización de Bibliotecas Koha**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de capacitación

Unidad de Documentación - Biblioteca			
Identificador único*	UDB-2		
(Nombre del sistema A1)*	**Formato de Registro de Usuarios de la Biblioteca**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de capacitación

Unidad de Docencia			
Identificador único*	UDC-1		
(Nombre del sistema A1)*	**Sistema de Registro para Participación en Eventos del CCM**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de capacitación

Dirección			
Identificador único*	DIR-1		
(Nombre del sistema A1)*	**Formato de Seguros**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, curso, material didáctico o recurso educativo para la capacitación. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de capacitación

8.2 Programa de difusión de la protección a los datos personales

Bienes y Suministros			
Identificador único*	ByS		
(Nombre del sistema A1)*	**Sistema Institucional de Compras**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de difusión para la protección de datos personales

Unidad Administrativa			
Identificador único*	UA-1		
(Nombre del sistema A1)*	**Sistema Integral de Personal. Expediente Físico**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de difusión para la protección de datos personales

Unidad Administrativa			
Identificador único*	UA-2		
(Nombre del sistema A1)*	**Expediente Físico Becarios Posdoctorales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de difusión para la protección de datos personales

Unidad Administrativa			
Identificador único*	UA-3		
(Nombre del sistema A1)*	**Expediente Físico de Prestadores de Servicios Profesionales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de difusión para la protección de datos personales

Unidad Administrativa			
Identificador único*	UA-4		
(Nombre del sistema A1)*	**Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de difusión para la protección de datos personales

Secretaría Académica			
Identificador único*	SA-1		
(Nombre del sistema A1)*	**Sistema para la Administración de Asuntos Académicos-Administrativos**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de difusión para la protección de datos personales

Secretaría Académica			
Identificador único*	SA-2		
(Nombre del sistema A1)*	**Sistema de Información Académica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de difusión para la protección de datos personales

Coordinación Administrativa del Posgrado de Matemáticas			
Identificador único*	PCCM-1		
(Nombre del sistema A1)*	**Sistema de ingreso para alumnos de posgrado**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de difusión para la protección de datos personales

Coordinación Administrativa del Posgrado de Matemáticas			
Identificador único*	PCCM-2		
(Nombre del sistema A1)*	**Sistema Integral de Administración Escolar del Posgrado**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de difusión para la protección de datos personales

Unidad de Documentación - Biblioteca			
Identificador único*	UDB-1		
(Nombre del sistema A1)*	**Sistema Integral de Automatización de Bibliotecas Koha**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de difusión para la protección de datos personales

Unidad de Documentación - Biblioteca			
Identificador único*	UDB-2		
(Nombre del sistema A1)*	**Formato de Registro de Usuarios de la Biblioteca**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de difusión para la protección de datos personales

Unidad de Docencia			
Identificador único*	UDC-1		
(Nombre del sistema A1)*	**Sistema de Registro para Participación en Eventos del CCM**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de difusión para la protección de datos personales

Asistente Dirección			
Identificador único*	DIR-1		
(Nombre del sistema A1)*	**Formato de Seguros**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Indique actividad, tema, recursos para la difusión. Agregar un renglón por cada elemento	*Describa el tipo de elemento, sus objetivos y forma de impartición, publicación o distribución*	*Indique duración del elemento en horas, días, meses, su fecha de inicio y de término*	*Mencione público objetivo, vigencia del elemento y frecuencia de actualización*

Actualmente no se cuenta con un programa de difusión para la protección de datos personales

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Bienes y Suministros			
Identificador único*	ByS		
(Nombre del sistema A1)*	**Sistema Institucional de Compras**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad Administrativa			
Identificador único*	UA-1		
(Nombre del sistema A1)*	**Sistema Integral de Personal. Expediente Físico**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad Administrativa			
Identificador único*	UA-2		
(Nombre del sistema A1)*	**Expediente Físico Becarios Posdoctorales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad Administrativa			
Identificador único*	UA-3		
(Nombre del sistema A1)*	**Expediente Físico de Prestadores de Servicios Profesionales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad Administrativa			
Identificador único*	UA-4		
(Nombre del sistema A1)*	**Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Secretaría Académica			
Identificador único*	SA-1		
(Nombre del sistema A1)*	**Sistema para la Administración de Asuntos Académicos-Administrativos**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Secretaría Académica			
Identificador único*	SA-2		
(Nombre del sistema A1)*	**Sistema de Información Académica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Aplicación de actualizaciones de seguridad	*Mantener al día en cuanto a las actualizaciones de seguridad disponibles el lenguaje de programación, framework de desarrollo y sistema operativo*	*Esta actividad es constante y permanente*	*Total, el sistema y sus dependencias se mantendrán actualizados según las actualizaciones de seguridad disponibles*

Coordinación Administrativa del Posgrado de Matemáticas			
Identificador único*	PCCM-1		
(Nombre del sistema A1)*	**Sistema de ingreso para alumnos de posgrado**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Coordinación Administrativa del Posgrado de Matemáticas			
Identificador único*	PCCM-2		
(Nombre del sistema A1)*	**Sistema Integral de Administración Escolar del Posgrado**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad de Documentación - Biblioteca			
Identificador único*	UDB-1		
(Nombre del sistema A1)*	**Sistema Integral de Automatización de Bibliotecas Koha**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad de Documentación - Biblioteca			
Identificador único*	UDB-2		
(Nombre del sistema A1)*	**Formato de Registro de Usuarios de la Biblioteca**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad de Docencia			
Identificador único*	UDC-1		
(Nombre del sistema A1)*	**Sistema de Registro para Participación en Eventos del CCM**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Aplicación de actualizaciones de seguridad	*Mantener al día en cuanto a las actualizaciones de seguridad disponibles el lenguaje de programación, framework de desarrollo y sistema operativo*	*Esta actividad es constante y permanente*	*Total, el sistema y sus dependencias se mantendrán actualizados según las actualizaciones de seguridad disponibles*

Asistente Dirección			
Identificador único*	DIR-1		
(Nombre del sistema A1)*	**Formato de Seguros**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

9.2 Actualización y mantenimiento de equipo de cómputo

Bienes y Suministros			
Identificador único*	ByS		
(Nombre del sistema A1)*	**Sistema Institucional de Compras**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad Administrativa			
Identificador único*	UA-1		
(Nombre del sistema A1)*	**Sistema Integral de Personal. Expediente Físico**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad Administrativa			
Identificador único*	UA-2		
(Nombre del sistema A1)*	**Expediente Físico Becarios Posdoctorales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad Administrativa			
Identificador único*	UA-3		
(Nombre del sistema A1)*	**Expediente Físico de Prestadores de Servicios Profesionales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad Administrativa			
Identificador único*	UA-4		
(Nombre del sistema A1)*	**Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Secretaría Académica			
Identificador único*	SA-1		
(Nombre del sistema A1)*	**Sistema para la Administración de Asuntos Académicos-Administrativos**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Secretaría Académica			
Identificador único*	SA-2		
(Nombre del sistema A1)*	**Sistema de Información Académica**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Coordinación Administrativa del Posgrado de Matemáticas			
Identificador único*	PCCM-1		
(Nombre del sistema A1)*	**Sistema de ingreso para alumnos de posgrado**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Coordinación Administrativa del Posgrado de Matemáticas			
Identificador único*	PCCM-2		
(Nombre del sistema A1)*	**Sistema Integral de Administración Escolar del Posgrado**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad de Documentación - Biblioteca			
Identificador único*	UDB-1		
(Nombre del sistema A1)*	**Sistema Integral de Automatización de Bibliotecas Koha**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad de Documentación - Biblioteca			
Identificador único*	UDB-2		
(Nombre del sistema A1)*	**Formato de Registro de Usuarios de la Biblioteca**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Unidad de Docencia			
Identificador único*	UDC-1		
(Nombre del sistema A1)*	**Sistema de Registro para Participación en Eventos del CCM**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

Asistente Dirección			
Identificador único*	DIR-1		
(Nombre del sistema A1)*	**Formato de Seguros**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
No aplica	*No aplica*	*No aplica*	*No aplica*

9.3 Procesos para la conservación, preservación y respaldos de información

Bienes y Suministros		
Identificador único*	ByS	
(Nombre del sistema A1)*	**Sistema Institucional de Compras**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*Dirección General de Proveeduría*

Unidad Administrativa		
Identificador único*	UA-1	
(Nombre del sistema A1)*	**Sistema Integral de Personal. Expediente Físico**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-2	
(Nombre del sistema A1)*	**Expediente Físico Becarios Posdoctorales**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-3	
(Nombre del sistema A1)*	**Expediente Físico de Prestadores de Servicios Profesionales**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-4	
(Nombre del sistema A1)*	**Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*No aplica*

Secretaría Académica		
Identificador único*	SA-1	
(Nombre del sistema A1)*	**Sistema para la Administración de Asuntos Académicos-Administrativos**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*Coordinación de la Investigación Científica*

Secretaría Académica		
Identificador único*	SA-2	
(Nombre del sistema A1)*	**Sistema de Información Académica**	
Proceso*	**Descripción***	**Responsable***
Los respaldos se encuentran en un equipo dedicado al almacenamiento de archivos de respaldo	*Cada uno de los respaldos realizados de la base de datos del sistema son almacenados y conservados manteniendo un histórico de archivos*	*Unidad de Cómputo*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-1	
(Nombre del sistema A1)*	**Sistema de ingreso para alumnos de posgrado**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*Dirección General de Administración Escolar*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-2	
(Nombre del sistema A1)*	**Sistema Integral de Administración Escolar del Posgrado**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*Dirección General de Administración Escolar*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-1	
(Nombre del sistema A1)*	**Sistema Integral de Automatización de Bibliotecas Koha**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*Dirección General de Bibliotecas y Servicios Digitales de Información*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-2	
(Nombre del sistema A1)*	**Formato de Registro de Usuarios de la Biblioteca**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad de Docencia		
Identificador único*	UDC-1	
(Nombre del sistema A1)*	**Sistema de Registro para Participación en Eventos del CCM**	
Proceso*	**Descripción***	**Responsable***
Los respaldos se encuentran en un equipo dedicado al almacenamiento de archivos de respaldo	*Cada uno de los respaldos realizados de la base de datos del sistema son almacenados y conservados manteniendo un histórico de archivos*	*Unidad de Cómputo*

Asistente Dirección		
Identificador único*	DIR-1	
(Nombre del sistema A1)*	**Formato de Seguros**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*No aplica*

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

Bienes y Suministros		
Identificador único*	ByS	
(Nombre del sistema A1)*	**Sistema Institucional de Compras**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*Dirección General de Proveeduría*

Unidad Administrativa		
Identificador único*	UA-1	
(Nombre del sistema A1)*	**Sistema Integral de Personal. Expediente Físico**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-2	
(Nombre del sistema A1)*	**Expediente Físico Becarios Posdoctorales**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-3	
(Nombre del sistema A1)*	**Expediente Físico de Prestadores de Servicios Profesionales**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad Administrativa		
Identificador único*	UA-4	
(Nombre del sistema A1)*	**Expediente Físico de Proyectos PAPIIT, PAPIME y CONACYT**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*No aplica*

Secretaría Académica		
Identificador único*	SA-1	
(Nombre del sistema A1)*	**Sistema para la Administración de Asuntos Académicos-Administrativos**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*Coordinación de la Investigación Científica*

Secretaría Académica		
Identificador único*	SA-2	
(Nombre del sistema A1)*	**Sistema de Información Académica**	
Proceso*	**Descripción***	**Responsable***
Herramientas dedicadas al borrado seguro de información	*Se utilizan herramientas para eliminar de forma segura la información de un medio de almacenamiento*	*Unidad de Cómputo*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-1	
(Nombre del sistema A1)*	**Sistema de ingreso para alumnos de posgrado**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*Dirección General de Administración Escolar*

Coordinación Administrativa del Posgrado de Matemáticas		
Identificador único*	PCCM-2	
(Nombre del sistema A1)*	**Sistema Integral de Administración Escolar del Posgrado**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*Dirección General de Administración Escolar*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-1	
(Nombre del sistema A1)*	**Sistema Integral de Automatización de Bibliotecas Koha**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*Dirección General de Bibliotecas y Servicios Digitales de Información*

Unidad de Documentación - Biblioteca		
Identificador único*	UDB-2	
(Nombre del sistema A1)*	**Formato de Registro de Usuarios de la Biblioteca**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*No aplica*

Unidad de Docencia		
Identificador único*	UDC-1	
(Nombre del sistema A1)*	**Sistema de Registro para Participación en Eventos del CCM**	
Proceso*	**Descripción***	**Responsable***
Herramientas dedicadas al borrado seguro de información	*Se utilizan herramientas para eliminar de forma segura la información de un medio de almacenamiento*	*Unidad de Cómputo*

Asistente Dirección		
Identificador único*	DIR-1	
(Nombre del sistema A1)*	**Formato de Seguros**	
Proceso*	**Descripción***	**Responsable***
No aplica	*No aplica*	*No aplica*

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

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

C) Medidas de seguridad para el bloqueo y posterior supresión del sistema DE TRATAMIENTO DE DATOS PERSONALES:

(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir las técnicas para la eliminación física del sistema)

Actualmente no se cuenta con un procedimiento para la cancelación de un sistema de tratamiento de datos personales.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	*MCC. Luis Gerardo Tejero Gómez, Técnico Académico de la Unidad de Cómputo* *Tel. 443 322 2777* *Ext Red UNAM. 42597* *gerardo@mamtor.unam.mx*	
Revisó:	*(Señalar nombre, puesto, teléfono y correo electrónico del funcionario o empleado universitario que revisó el documento de seguridad)*	
Autorizó:	(*Señalar nombre, puesto, teléfono y correo electrónico del funcionario o empleado universitario que autorizó el documento de seguridad)*	
Fecha de aprobación:	(Incluir la fecha de liberación del documento)	
Fecha de actualización:	(Incluir la primer versión e ir agregando las subsiguientes del documento)	