



CENTRO DE INVESTIGACIONES
Y ESTUDIOS DE GÉNERO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

CENTRO DE INVESTIGACIONES Y ESTUDIOS DE GÉNERO

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

2026

TABLA DE CONTENIDO

PRESENTACIÓN	4
OBJETIVO	4
ALCANCE	4
SISTEMAS DE TRATAMIENTOS DE DATOS PERSONALES	4
SISTEMAS INTERNOS	7
Sistema de videovigilancia	7
1. Inventario de Sistemas de Tratamientos de Datos Personales	7
2. Estructura y descripción de los Sistemas de Tratamiento de Datos Personales	9
3. Análisis de riesgos	9
4. Análisis de brecha	10
5. Plan de trabajo	10
6. Medidas de seguridad implementadas	11
7. Mecanismos de monitoreo y revisión de las medidas de seguridad	14
8. Programa específico de capacitación	15
9. Mejora continua	15
10. Procedimiento para la cancelación de un Sistema de Tratamiento de Datos Personales	17
Sistema de Control de Acceso	18
1. Inventario de Sistemas de Tratamientos de Datos Personales	18
2. Estructura y descripción de los Sistemas de Tratamiento de Datos Personales	19
3. Análisis de riesgos	19
4. Análisis de brecha	20
5. Plan de trabajo	20
6. Medidas de seguridad implementadas	21
7. Mecanismos de monitoreo y revisión de las medidas de seguridad	25
8. Programa específico de capacitación	26
9. Mejora continua	26
10. Procedimiento para la cancelación de un Sistema de Tratamiento de Datos Personales	27
Sistema Interno de Informes	28
1. Inventario de Sistemas de Tratamientos de Datos Personales	28
2. Estructura y descripción de los Sistemas de Tratamiento de Datos Personales	30
3. Análisis de riesgos	30
4. Análisis de brecha	31
5. Plan de trabajo	31
6. Medidas de seguridad implementadas	32
7. Mecanismos de monitoreo y revisión de las medidas de seguridad	36
8. Programa específico de capacitación	37

9. Mejora continua	37
10. Procedimiento para la cancelación de un Sistema de Tratamiento de datos personales	39
SITIO WEB	40
1. Inventario de Sistemas de Tratamientos de Datos Personales	40
2. Estructura y descripción de los Sistemas de Tratamiento de Datos Personales	42
3. Análisis de riesgos	43
4. Análisis de brecha	44
5. Plan de trabajo	44
6. Medidas de seguridad implementadas	45
7. Mecanismos de monitoreo y revisión de las medidas de seguridad	49
8. Programa específico de capacitación	50
9. Mejora continua	50
10. Procedimiento para la cancelación de un Sistema de Tratamiento de datos personales	52
SISTEMAS TRANSVERSALES	53
Sistema Integral de Personal	53
Módulo de Servicios Profesionales	56
Nómina institucional UNAM	58
Estímulos UNAM	59
Trámite de Pago por Otros Servicios del Personal UNAM	61
Sistema de Administración Institucional	62
Aplicaciones DGPO	80
Sistema Integral de Administración Financiera	84
Sistema Integral de Control Patrimonial	85
Portal Patronato	86
Módulo de Factura Digital UNAM	87
Sistema de Evaluación de Concursos de Oposición Abiertos	88
Sistema de Informes Académicos del Subsistema de Humanidades	90
Sistema de Gestión Electrónica	92
Sistema Integral de Estímulo por Asistencia al Personal Académico de la UNAM	94
Sistema de Elecciones de la Dirección General de Personal	95
Sistema de gestión Koha	97
Directorio Universitario	98
Sistema Ápeiron	99
Aprobación del Documento de seguridad	102

PRESENTACIÓN

La protección de los datos personales constituye una obligación institucional sustentada en la Constitución Política de los Estados Unidos Mexicanos y en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. En el ámbito universitario, esta obligación se desarrolla en el Acuerdo por el que se establecen los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México y en las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, así como en la demás normatividad universitaria aplicable.

En este contexto, el Centro de Investigaciones y Estudios de Género (CIEG) de la Universidad Nacional Autónoma de México implementa medidas orientadas a preservar la confidencialidad, integridad y disponibilidad de la información, así como a prevenir el acceso, uso, modificación o divulgación no autorizados.

Con este propósito, el presente Documento de Seguridad establece las medidas administrativas, físicas y técnicas aplicables al tratamiento de datos personales en el CIEG. Asimismo, identifica las áreas responsables, define las responsabilidades de las personas servidoras universitarias que intervienen en su tratamiento y establece las medidas generales para su protección, en apego a la normatividad vigente.

OBJETIVO

Establecer las medidas administrativas, físicas y técnicas, así como las responsabilidades de las áreas competentes, para garantizar la protección de los datos personales tratados por el CIEG, de conformidad con la legislación y la normatividad universitaria aplicables.

ALCANCE

El presente Documento de Seguridad es aplicable a las personas titulares de la Dirección, las Secretarías y los Departamentos del CIEG que, por razón de sus atribuciones, intervengan en el tratamiento de datos personales o sean responsables de sistemas que contengan dicha información.

SISTEMAS DE TRATAMIENTOS DE DATOS PERSONALES

Para el desarrollo de sus funciones académico-administrativas, el CIEG utiliza diversos sistemas informáticos y tecnológicos que requieren el tratamiento de datos personales de integrantes de la comunidad universitaria, personas prestadoras de servicios, proveedoras y proveedores, así como de personas usuarias y visitantes. Estos sistemas se clasifican en dos categorías:

Sistemas internos:

- Sistema de videovigilancia (CCTV): sistema de monitoreo mediante cámaras de videovigilancia destinado a fortalecer la seguridad de las personas, así como la protección de las instalaciones y los bienes institucionales.
- Sistema de Control de Acceso (SCA): sistema utilizado para registrar y controlar el ingreso a las instalaciones del CIEG mediante tarjeta de identificación universitaria (RIF) o autenticación biométrica por huella dactilar.
- Sistema Interno de Informes: sistema utilizado por el personal académico y administrativo para registrar trimestralmente las actividades desarrolladas durante el año.
- Sitio web institucional (WEB): plataforma digital destinada a la difusión de información sobre las actividades, proyectos y servicios del CIEG, que permite, en su caso, la recopilación de datos personales mediante formularios de contacto o registro habilitados para las personas usuarias.

Sistemas transversales:

- Sistema Integral de Personal
- Módulo de Servicios Profesionales
- Nómina Institucional UNAM
- Estímulos UNAM
- Trámite de Pago por Otros Servicios del Personal UNAM
- Sistema de Administración Institucional
- Aplicaciones DGPO
- Sistema Integral de Administración Financiera
- Sistema Integral de Control Patrimonial
- Portal Patronato
- Módulo de Factura Digital UNAM
- Sistema de Evaluación de Concursos de Oposición Abiertos
- Sistema de Informes Académicos del Subsistema de Humanidades
- Sistema de Gestión y Estímulos Académicos
- Sistema de Gestión Electrónica
- Sistema Integral de Estímulo por Asistencia al Personal Académico de la UNAM
- Sistema de Elecciones de la Dirección General de Personal
- Sistema de Gestión Koha
- Directorio Universitario
- Sistema Ápeiron

SISTEMAS INTERNOS

SISTEMA DE VIDEOVIGILANCIA

1. Inventario de Sistemas de Tratamientos de Datos Personales

CIEG Departamento de Tecnologías de la Información y Comunicaciones	
Identificador único	CIEG/CCTV
Nombre del sistema	Monitoreo CCTV
Datos personales (sensibles o no) contenidos en el sistema	Datos de identificación: imagen de una persona identificada, fecha y hora de ingreso, fecha y hora de salida.

Responsable	
Nombre	Servando Arturo Jiménez Colín
Cargo	Jefe del Departamento de Tecnologías de la Información y Comunicaciones
Funciones	<ul style="list-style-type: none"> • Administrar el equipo de CCTV (cámaras, grabadoras, servidores y monitores). • Verificar el funcionamiento continuo del sistema y asegurar el correcto almacenamiento de las grabaciones. • Realizar mantenimientos preventivos y correctivos para asegurar el funcionamiento y rendimiento óptimo de los equipos de CCTV. • Crear usuarios/encargados para acceso a las cámaras del CCTV y asignar permisos con base en su nivel de acceso. • Registrar y reportar incidentes y brindar las grabaciones cuando sean solicitadas por el personal autorizado. • Asegurar el cumplimiento de normativas y políticas internas sobre videovigilancia.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales.

	<ul style="list-style-type: none"> • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
--	---

Encargada/Usuaría	
Nombre	Marlene Carolina Pérez Limón
Cargo	Secretaria Administrativa
Funciones	<ul style="list-style-type: none"> • Consultar las grabaciones del Sistema de Videovigilancia únicamente cuando exista una necesidad institucional debidamente justificada, como la atención de incidentes, investigaciones administrativas o requerimientos de autoridades competentes. • Autorizar la revisión de las grabaciones cuando sea solicitada por las áreas competentes y exista un motivo debidamente documentado. • Dar seguimiento a los incidentes reportados que requieran la revisión de las grabaciones para apoyar la aclaración de los hechos o la integración de la documentación correspondiente. • Coordinar con el Departamento de Tecnologías de la Información y Comunicaciones (DTIC) la atención de fallas que afecten el funcionamiento del Sistema de Videovigilancia. • Solicitar al DTIC la recuperación de grabaciones cuando sea necesario atender incidentes institucionales o requerimientos legalmente procedentes. • Validar que las cámaras instaladas continúen cumpliendo con las necesidades operativas y reportar cuando se identifiquen zonas sin cobertura o deficiencias en la vigilancia.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente.

	<ul style="list-style-type: none"> No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
--	--

2. Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

CIEG Departamento de Tecnologías de la Información y Comunicaciones	
Identificador único	CIEG/CCTV
Nombre del sistema	Monitoreo CCTV
Tipo de soporte	Físico y electrónico
Descripción	El sistema posee un DVR (Digital Video Recorder) que se utiliza para almacenar las grabaciones por un tiempo determinado, dichas grabaciones se obtienen mediante comunicación Ethernet de las cámaras al servidor.
Características del lugar donde se resguardan los soportes:	El equipo se resguarda en un <i>site</i> que se encuentra bajo llave, al cual tiene acceso la persona responsable. Dicho <i>site</i> se encuentra en una sala con chapa de seguridad a la que se accede con una llave y el permiso de vigilancia.

3. Análisis de riesgos

CENTRO DE INVESTIGACIONES
Y ESTUDIOS DE GÉNERO

	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED] [REDACTED]	[REDACTED]	[REDACTED] [REDACTED]

4. Análisis de brecha

[illegible]

5. Plan de trabajo

[illegible]

6. Medidas de seguridad implementadas

6.1. Transferencias de datos personales

CIEG Departamento de Tecnologías de la Información y Comunicaciones	
Identificador único	CIEG/CCTV
Nombre del sistema	Monitoreo CCTV
Transferencia de Datos Personales	
Transferencias mediante el traslado de soportes físicos	No Aplica
Transferencias mediante el traslado de soportes electrónicos	No Aplica
Transferencias mediante el traslado sobre redes electrónicas	No Aplica

6.2. Resguardo de sistemas de tratamiento de datos personales con soportes físicos

El equipo se encuentra resguardado dentro de un *site* cuyo acceso permanece restringido y bajo llave. El ingreso al *site* está limitado al personal responsable y autorizado para realizar actividades de administración, mantenimiento o supervisión de los equipos. Asimismo, el *site* se encuentra ubicado dentro de una sala que cuenta con chapa de seguridad, cuyo acceso requiere el uso de una llave y la autorización del personal de vigilancia. Estas medidas permiten restringir el acceso físico a los equipos, prevenir su manipulación por personas no autorizadas y reducir riesgos de daño, pérdida, alteración o acceso indebido a la infraestructura y a la información que ésta soporta.

Acceso a los soportes físicos del sistema

Nombre: Servando Arturo Jiménez Colín

Cargo: Jefe del Departamento de Tecnologías de la Información y Comunicaciones

Funciones:

- Administrar el equipo de CCTV (cámaras, grabadoras, servidores y monitores)
- Verificar el funcionamiento continuo del sistema y asegurar el correcto almacenamiento de las grabaciones
- Realizar mantenimientos preventivos y correctivos para asegurar el funcionamiento y rendimiento óptimo de los equipos de CCTV
- Crear usuarios/encargados para acceso a las cámaras del CCTV y asignar permisos con base en su nivel de acceso
- Registrar y reportar incidentes y brindar las grabaciones cuando sean

solicitadas por el personal autorizado

- Asegurar el cumplimiento de normativas y políticas internas sobre videovigilancia

Obligaciones:

- Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones
- Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables
- Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados
- Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente.
- No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales
- Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente
- Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales
- Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales

6.3. Bitácoras para accesos y operación cotidiana

No aplica.

6.4. Registro de incidentes

El personal que haya notado el incidente, debe dirigirse a la persona responsable de DTIC que determinará la mejor acción necesaria para solucionar la incidencia y atenderla.

6.5. Acceso a las instalaciones

- Seguridad perimetral exterior: La entrada principal de la Torre II de Humanidades cuenta con acceso controlado a cargo del personal de vigilancia UNAM. Asimismo, se cuenta con videovigilancia las 24 horas en pasillos. Las personas externas que accedan a la Torre deben emitir un registro en bitácora indicando área, piso y persona que visitan, así como la hora de entrada y de salida.
- Seguridad perimetral interior: En la entrada principal del CIEG en el piso 7 de la Torre II de Humanidades también se cuenta con acceso controlado, ya que para poder ingresar a las oficinas debe permitirse la entrada por personal de vigilancia. Se cuenta con videovigilancia las 24 horas en pasillos y demás áreas de las instalaciones. Las personas externas que accedan a la Torre

deben emitir un registro en bitácora indicando área, piso y persona que visitan, así como la hora de entrada y salida.

6.6. Actualización de la información contenida en el sistema de tratamiento de datos personales

En caso de requerir una actualización de datos personales, la persona interesada debe dirigirse al DTIC donde se determinará el tipo de proceso a seguir para realizar el cambio requerido.

6.7. Perfiles de usuario y contraseñas

I. Modelo de control de acceso

El modelo de control de acceso utilizado es discrecional, ya que los permisos son asignados por una persona administradora, además de estar basado en reglas y roles.

II. Perfiles de usuario y contraseñas en el sistema operativo de red

No Aplica.

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

No Aplica.

IV. Administración de perfiles de usuario y contraseñas

La persona titular del Departamento de Tecnologías de la Información y Comunicaciones es quien gestiona la administración de los perfiles y realiza el procedimiento correspondiente.

V. Acceso remoto al sistema de tratamiento de datos personales

No Aplica.

6.8. Procedimiento de respaldo y recuperación de datos

Señalar si realiza respaldos:

- Completos ☒X___, diferenciales ___ o incrementales ___
- De forma automática ☒X___ o Manual _____
- Periodicidad: ___1 año aproximadamente ___
- Tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Se utiliza un disco duro.

- Cómo y dónde se archivan esos medios: En la unidad de almacenamiento incluida en el DVR.
- Quién es la persona responsable de realizar estas operaciones (el área universitaria o una tercera persona): Los respaldos se realizan en su totalidad por el sistema de manera automática; son resguardados por la persona titular del DTIC.

6.9. Plan de contingencia

Ante situaciones que puedan afectar el funcionamiento de las cámaras, DVR, suministro eléctrico, conectividad de red o demás componentes asociados, se cuenta con un plan de contingencia para atender las incidencias que puedan presentarse. Inicialmente, se identifica la causa de la interrupción y se verifica el estado de los equipos, conexiones y alimentación eléctrica. Cuando resulta procedente, se lleva a cabo un reinicio controlado del DVR y de los equipos asociados para restablecer su funcionamiento. Si la falla persiste, se solicita al proveedor especializado la atención correspondiente, incluyendo acciones de mantenimiento, reparación o sustitución de los componentes afectados. Una vez restablecido el servicio, se verifica el correcto funcionamiento de las cámaras, la grabación y el almacenamiento de las imágenes.

La recuperación se realiza sobre la infraestructura principal mediante el personal responsable y, cuando corresponde, con apoyo del proveedor especializado. El tiempo de restablecimiento depende del tipo de falla y de la disponibilidad de los equipos o servicios necesarios para su reparación o sustitución.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/CCTV	
Nombre del sistema	Monitoreo CCTV	
Recurso	Descripción	Control
No Aplica	No Aplica	No Aplica

7.2. Procedimiento para la revisión de las medidas de seguridad

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/CCTV	
Nombre del sistema	Monitoreo CCTV	
Medida de seguridad	Procedimiento	Responsable
No Aplica	No Aplica	No Aplica

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones	
Identificador único	CIEG/CCTV
Nombre del sistema	Monitoreo CCTV

Medida de seguridad	Procedimiento	Responsable
No Aplica	No Aplica	No Aplica

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/CCTV	
Nombre del sistema	Monitoreo CCTV	
Medida de seguridad	Procedimiento	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

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/CCTV		
Nombre del sistema	Monitoreo CCTV		
Actividad	Descripción	Duración	Cobertura
No Aplica	No Aplica	No Aplica	No Aplica

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/CCTV		
Nombre del sistema	Monitoreo CCTV		
Actividad	Descripción	Duración	Cobertura
No Aplica	No Aplica	No Aplica	No Aplica

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/CCTV		
Nombre del sistema	Monitoreo CCTV		
Actividad	Descripción	Duración	Cobertura
No Aplica	No Aplica	No Aplica	No Aplica

9.2. Actualización y mantenimiento de equipo de cómputo

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/CCTV		
Nombre del sistema	Monitoreo CCTV		
Actividad	Descripción	Duración	Cobertura
Mantenimiento	Mantenimiento para el sistema CCTV mediante proveedor.	6-8 horas semestralmente.	Garantizar la disponibilidad y correcto funcionamiento de la infraestructura

			de videovigilancia mediante acciones preventivas que permitan detectar fallas y prolongar la vida útil de los equipos.
Actualización	Adquisición de equipo y cambios de cámaras y/o software mediante proveedor.	6-8 horas semestralmente.	Mantener la infraestructura actualizada, confiable y compatible con los requerimientos de operación y seguridad institucional.

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/CCTV	
Nombre del sistema	Monitoreo CCTV	
Medida de seguridad	Procedimiento	Responsable
Respaldo físico de las grabaciones	Conexión al DVR y descarga del archivo en computadora específica para almacenamiento	Servando Arturo Jiménez Colín Jefe del Departamento de TIC

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/CCTV	
Nombre del sistema	Monitoreo CCTV	
Medida de seguridad	Procedimiento	Responsable
Borrado de archivos	Eliminación de archivos directamente en el servidor DVR y copias almacenadas mediante conexión física al servidor y unidades de almacenamiento. Formateo de unidades de almacenamiento y entrega al Departamento de Bienes y Suministros para eliminación y baja del sistema.	Servando Arturo Jiménez Colín Jefe del Departamento de TIC

10. Procedimiento para la cancelación de un Sistema de Tratamiento de Datos Personales

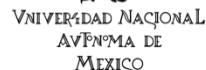
En caso de requerir una cancelación, la persona interesada debe dirigirse a la persona responsable del DTIC para determinar si puede hacer la cancelación de la información o especificar qué proceso debe realizar para el cambio que requiere.

Los datos personales únicamente serán cancelados cuando dejen de ser necesarios para el cumplimiento de su finalidad. Una vez que fue autorizada la cancelación del sistema deben ser identificados los datos personales y bloqueados de tal forma que el acceso a ellos esté cancelado y solo puedan ser consultados bajo obligaciones legales. Posteriormente, se aplicarán mecanismos para la supresión de estos datos personales, este procedimiento comprenderá la validación de la autorización para la eliminación del sistema, la desinstalación del aplicativo cuando corresponda, la eliminación de la base de datos y de las copias de seguridad que hayan concluido su periodo de conservación, la eliminación de la configuración almacenada en el DVR y la documentación de todas las actividades realizadas mediante el registro correspondiente.

SISTEMA DE CONTROL DE ACCESO

1. Inventario de Sistemas de Tratamientos de Datos Personales

CIEG Departamento de Tecnologías de la Información y Comunicaciones	
Identificador único	CIEG/SCA
Nombre del sistema	Sistema de Control de Acceso
Datos personales (sensibles o no) contenidos en el sistema	Datos de identificación: Datos biométricos de huella digital. Datos personales: Nombre del trabajador o trabajadora, dependencia de adscripción
Responsable	
Nombre	Servando Arturo Jiménez Colín
Cargo	Jefe del Departamento de Tecnologías de la Información y Comunicaciones
Funciones	<ul style="list-style-type: none"> • Administrar y supervisar el Sistema de Control de Acceso para su correcto funcionamiento y disponibilidad. • Autorizar, registrar, modificar y revocar los permisos de acceso de las personas usuarias, conforme a las autorizaciones emitidas por las respectivas áreas. • Supervisar el proceso de enrolamiento biométrico, verificando que la captura de huellas dactilares se realice conforme a los procedimientos establecidos y con las medidas de seguridad correspondientes. • Vigilar la confidencialidad, integridad y disponibilidad de la información contenida en el sistema, implementando las medidas necesarias para su protección. • Monitorear los registros de acceso y las bitácoras del sistema para identificar accesos no autorizados, anomalías o posibles incidentes de seguridad. • Supervisar que el acceso a la información y a las bases de datos del sistema sea exclusivo del personal previamente autorizado. • Realizar el mantenimiento preventivo de los equipos biométricos para asegurar su correcto funcionamiento.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.



- | | |
|--|--|
| | <ul style="list-style-type: none"> • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales. |
|--|--|

Persona a cargo /Usuaria/o	
Nombre	No Aplica
Cargo	No Aplica
Funciones	No Aplica
Obligaciones	No Aplica

2. Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

CIEG Departamento de Tecnologías de la Información y Comunicaciones	
Identificador único	CIEG/SCA
Nombre del sistema	Sistema de Control de Acceso
Tipo de soporte	Físico y electrónico
Descripción	La información biométrica y los registros de acceso son gestionados por el software del sistema, desde el cual pueden generarse reportes en distintos formatos para fines administrativos y de seguimiento.
Características del lugar donde se resguardan los soportes:	Los soportes electrónicos son resguardados en el equipo de cómputo y en un servidor donde se encuentra instalado el software de administración del Sistema de Control de Acceso. El acceso a la información está restringido al personal autorizado mediante mecanismos de autenticación y controles de seguridad físicos y lógicos.

3. Análisis de riesgos



[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

4. Análisis de brecha

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

5. Plan de trabajo

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

6. Medidas de seguridad implementadas

6.1. Transferencias de datos personales

CIEG Departamento de Tecnologías de la Información y Comunicaciones	
Identificador único	CIEG/SCA
Nombre del sistema	Sistema de Control de Acceso
Transferencia de Datos Personales	
Transferencias mediante el traslado de soportes físicos	No Aplica
Transferencias mediante el traslado de soportes electrónicos	No Aplica
Transferencias mediante el traslado sobre redes electrónicas	No Aplica

6.2. Resguardo de sistemas de tratamiento de datos personales con soportes físicos

El equipo que contiene el software para poder acceder a las terminales biométricas de Control de Acceso, los cuales se encuentran ubicados en un área segura constantemente vigilada tanto por personal de seguridad como por medio de cámaras de seguridad perteneciente al sistema CCTV así como autenticación biométrica.

Acceso a los soportes físicos del sistema

Nombre: Servando Arturo Jiménez Colín

Cargo: Jefe del Departamento de Tecnologías de la Información y Comunicaciones

Funciones:

- Administrar y supervisar el Sistema de Control de Acceso para su correcto funcionamiento y disponibilidad.
- Autorizar, registrar, modificar y revocar los permisos de acceso de las personas usuarias, conforme a las autorizaciones emitidas por las respectivas áreas.
- Supervisar el proceso de enrolamiento biométrico, verificando que la captura de huellas dactilares se realice conforme a los procedimientos establecidos y con las medidas de seguridad correspondientes.
- Vigilar la confidencialidad, integridad y disponibilidad de la información contenida en el sistema, implementando las medidas necesarias para su protección.
- Monitorear los registros de acceso y las bitácoras del sistema para identificar accesos no autorizados, anomalías o posibles incidentes de seguridad.
- Supervisar que el acceso a la información y a las bases de datos del sistema sea exclusivo del personal previamente autorizado.
- Realizar el mantenimiento preventivo de los equipos biométricos para asegurar su correcto funcionamiento.

Obligaciones:

- Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones.
- Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables.
- Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.
- Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente.
- No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales.
- Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente.
- Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales.
- Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

6.3. Bitácoras para accesos y operación cotidiana

Los datos que se registran en las bitácoras:

- Son de acceso exclusivo del personal autorizado.

- Las bitácoras se almacenan en soporte electrónico. El aplicativo puede registrar acciones como altas, bajas y modificaciones de usuarios, asignación de permisos, registro o eliminación de plantillas biométricas, cambios de configuración, sincronización con terminales, consultas y exportación de reportes.
- Las bitácoras generalmente se almacenan en la base de datos del aplicativo instalada en el servidor o equipo que administra el sistema. El tiempo de conservación es de aproximadamente un año o hasta que sean borradas por el mismo sistema o por una persona administradora.
- La integridad de las bitácoras se asegura mediante controles de acceso al aplicativo y a la base de datos, autenticación de usuarios, restricciones de permisos, respaldos periódicos.
- El área responsable de la administración del sistema de control de acceso es el Departamento de Tecnologías de la Información y Comunicaciones de la Información, el cual realiza revisiones mensuales y, en caso de que ocurra un incidente, se hace una revisión extraordinaria.
- El análisis de las bitácoras electrónicas se realiza mediante el módulo de generación de reportes del software, también de ser necesario se utilizan herramientas como Microsoft Excel para el análisis de los registros exportados.

6.4. Registro de incidentes

El personal que haya notado el incidente, debe dirigirse a la persona responsable de DTIC que determinará la mejor acción necesaria para solucionar la incidencia y atenderla.

6.5. Acceso a las instalaciones

- Seguridad perimetral exterior: En la entrada principal de edificio de la Torre II de Humanidades se cuenta con acceso controlado, puesto que para poder ingresar al edificio debe permitirse la entrada por personal de vigilancia UNAM, además de contar con videovigilancia las 24 horas en pasillos y demás áreas de las instalaciones. Se lleva un registro de las personas externas detallando el área donde se dirigen, el piso y el funcionario que visita, así como la hora de entrada y de salida.
- Seguridad perimetral interior: En la entrada principal del CIEG también se cuenta con acceso controlado, ya que para poder ingresar a las oficinas debe permitirse la entrada por personal de vigilancia, además de contar con videovigilancia las 24 horas en pasillos y demás áreas de las instalaciones. Se lleva un registro de las personas externas detallando el nombre, motivo de la visita, hora de entrada y salida, así como identificar a la persona con quien se tiene programada la visita en la institución.

6.6. Actualización de la información contenida en el sistema de tratamiento de datos personales

Para el cambio o actualización de la información debe ser requerido por la persona titular correspondiente o por la persona representante de las y los trabajadores de la dependencia al jefe del DTIC quien valorará y atenderá la petición siguiendo el protocolo correspondiente.

6.7. Perfiles de usuario y contraseñas

I. Modelo de control de acceso

El modelo de control de acceso utilizado es discrecional, ya que los permisos son asignados por una persona administrador, además de estar basado en reglas y roles.

II. Perfiles de usuario y contraseñas en el sistema operativo de red

El equipo en donde se encuentra el software aplicativo no cuenta con un sistema operativo de red.

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

El software del aplicativo cuenta con un manejo de perfiles y permisos dependiendo del privilegio asignado para que no cualquiera pueda modificar la información y configuraciones, además de tener que autenticarse mediante usuario y contraseña.

Si se almacenan los nombres de usuario, así como sus respectivas contraseñas mediante un cifrado de datos que no se puede invertir.

IV. Administración de perfiles de usuario y contraseñas

La persona titular del Departamento de Tecnologías de la Información y Comunicaciones es quien gestiona la administración de los perfiles y realiza el procedimiento correspondiente.

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

No se permite el acceso remoto en los equipos de cómputo en los que se trabaja el sistema.

6.8. Procedimiento de respaldo y recuperación de datos

Señalar si realiza respaldos:

- Completos X , diferenciales o incrementales
- De forma automática o Manual X
- Periodicidad con que los realiza: mensual.

- El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: se utiliza un disco duro.
- Cómo y dónde se archivan esos medios: en la unidad de almacenamiento externa.
- Quién es la persona responsable de realizar estas operaciones (el área universitaria o una tercera persona): los respaldos son realizados por la persona responsable del DTIC.

6.9. Plan de contingencia

Se cuenta con un plan de contingencia en el cual se establecen las acciones que deberán seguirse para atender fallas en el equipo de cómputo, interrupciones del suministro de energía eléctrica, pérdida de conectividad con la red institucional, daños en las terminales biométricas, fallas del aplicativo o de la base de datos.

Como primera acción a realizar se verifica la disponibilidad e integridad de las copias de seguridad, después se identifican los componentes necesarios para la restauración del servicio incluyendo el sistema operativo, el aplicativo, la base de datos y sus respectivas configuraciones. Posteriormente, se procede a la recuperación de la información utilizando los respaldos más recientes disponibles para finalmente realizar la documentación técnica necesaria para la reinstalación y configuración del sistema, la participación del personal responsable del DTIC durante el proceso de recuperación y la validación del correcto funcionamiento del aplicativo y de las terminales biométricas antes de restablecer el servicio. Cuando se concluye el proceso de recuperación se verifica que todo funciona de forma adecuada para finalmente documentar el incidente.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/SCA	
Nombre del sistema	Sistema de Control de Acceso	
Recurso	Descripción	Control
No Aplica	No Aplica	No Aplica

7.2. Procedimiento para la revisión de las medidas de seguridad

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/SCA	
Nombre del sistema	Sistema de Control de Acceso	
Medida de seguridad	Procedimiento	Responsable
No Aplica	No Aplica	No Aplica

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/SCA	
Nombre del sistema	Sistema de Control de Acceso	
Medida de seguridad	Procedimiento	Responsable
No Aplica	No Aplica	No Aplica

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/SCA	
Nombre del sistema	Sistema de Control de Acceso	
Medida de seguridad	Procedimiento	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

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/SCA		
Nombre del sistema	Sistema de Control de Acceso		
Actividad	Descripción	Duración	Cobertura
No Aplica	No Aplica	No Aplica	No Aplica

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/SCA		
Nombre del sistema	Sistema de Control de Acceso		
Actividad	Descripción	Duración	Cobertura
No Aplica	No Aplica	No Aplica	No Aplica

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/SCA		
Nombre del sistema	Sistema de Control de Acceso		
Actividad	Descripción	Duración	Cobertura
Actualización y mejora del software aplicativo	Se identifican e instalan las versiones más recientes del software aplicativo.	3 a 4 hrs	Actualizaciones tanto del sistema operativo como de la versión del aplicativo y sus componentes.

9.2. Actualización y mantenimiento de equipo de cómputo

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/SCA		
Nombre del sistema	Sistema de Control de Acceso		
Actividad	Descripción	Duración	Cobertura
Mantenimiento preventivo	Actualización de firmware y revisión terminales de biometricos.	2 - 4 hrs	Verificación del buen funcionamiento de las terminales de biométricos y de la comunicación con el software aplicativo.
Actualización del sistema operativo y del aplicativo de control de acceso	Instalación de actualizaciones del sistema operativo y de los parches o versiones compatibles del aplicativo de administración del sistema de control de acceso.	6 - 8 hrs	Corrección de vulnerabilidades y mejora de la estabilidad del sistema.

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/SCA	
Nombre del sistema	Sistema de Control de Acceso	
Medida de seguridad	Procedimiento	Responsable
Respaldo de la base de datos con los registros y bitácoras de entrada	Se realiza un respaldo de la base de datos del aplicativo de control de acceso biométrico, este se genera utilizando las herramientas disponibles del aplicativo realizando una copia en el mismo equipo.	Servando Arturo Jiménez Colín Jefe del Departamento de TIC

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/SCA	
Nombre del sistema	Sistema de Control de Acceso	
Medida de seguridad	Procedimiento	Responsable
Borrado seguro en equipos de cómputo donde está alojado el software aplicativo	Antes de reutilizar, reasignar o dar de baja el equipo de cómputo se realiza el borrado seguro de	Servando Arturo Jiménez Colín Jefe del Departamento de TIC

	la información almacenada mediante herramientas especializadas que sobrescriben el contenido del dispositivo de almacenamiento, evitando la recuperación de datos personales y de la configuración del sistema.	
Borrado seguro en terminales biometricas	Al sustituir o retirar una terminal biométrica se eliminan previamente las configuraciones, registros, así como la información almacenada en el dispositivo. Posteriormente, el equipo es retirado del inventario institucional.	Servando Arturo Jiménez Colín Jefe del Departamento de TIC

10. Procedimiento para la cancelación de un Sistema de Tratamiento de Datos Personales

Dado que se trata de un sistema utilizado por diversas dependencias universitarias, el procedimiento para su cancelación debe ser mediante un acuerdo entre las personas titulares de las unidades administrativas y de las personas titulares de las diversas dependencias.

El sistema de tratamiento de datos únicamente será cancelado cuando deje de ser necesario para el cumplimiento de su finalidad. Una vez que fue autorizada la cancelación del sistema, deben ser identificados los datos personales y bloqueados de tal forma que el acceso a ellos sea cancelado y solo puedan ser consultados bajo obligaciones legales. Posteriormente, se aplicarán mecanismos para la supresión de estos datos personales, este procedimiento comprenderá la validación de la autorización para la eliminación del sistema, la desinstalación del aplicativo cuando corresponda, la eliminación de la base de datos y de las copias de seguridad que hayan concluido su periodo de conservación, la eliminación de la configuración almacenada en las terminales biométricas y la documentación de todas las actividades realizadas mediante el registro correspondiente.

SISTEMA INTERNO DE INFORMES

1. Inventario de Sistemas de Tratamientos de Datos Personales

CIEG Departamento de Tecnologías de la Información y Comunicaciones	
Identificador único	CIEG/SII
Nombre del sistema	Sistema Interno de Informes
Datos personales (sensibles o no) contenidos en el sistema	<p>Datos de identificación: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad.</p> <p>Datos laborales: Nombramiento, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, entre otros.</p> <p>Datos académicos: Nivel de estudios, cédula profesional.</p>

Responsable	
Nombre	Servando Arturo Jiménez Colín
Cargo	Jefe del Departamento de Tecnologías de la Información y Comunicaciones
Funciones	<ul style="list-style-type: none"> Dirigir y supervisar la operación del Sistema de Informes, asegurando que funcione de manera continua, eficiente y conforme a las necesidades institucionales. Supervisar el cumplimiento de las políticas, lineamientos y procedimientos relacionados con el tratamiento y protección de los datos personales contenidos en el sistema. Coordinar las actividades de mantenimiento preventivo y correctivo del aplicativo, la infraestructura tecnológica y la base de datos que soportan el Sistema de Informes. Autorizar y supervisar la implementación de actualizaciones del sistema, verificando previamente su compatibilidad y minimizando el impacto en la operación institucional. Promover la mejora continua del Sistema de Informes mediante la evaluación periódica de su desempeño, disponibilidad, seguridad y cumplimiento de los objetivos institucionales.
Obligaciones	<ul style="list-style-type: none"> Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.

	<ul style="list-style-type: none"> • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
--	--

Encargada/Usuaría	
Nombre	Gabriela Sánchez Flores
Cargo	Jefa del Área de Planeación
Funciones	<ul style="list-style-type: none"> • Utilizar el Sistema de Informes para registrar, consultar, actualizar y dar seguimiento a la información correspondiente a sus actividades, conforme a los procedimientos institucionales. • Verificar que la información capturada en el Sistema de Informes sea completa, veraz, oportuna y corresponda a la documentación o evidencia que la respalda. • Dar seguimiento a las actividades registradas en el sistema para verificar el avance de los procesos y el cumplimiento de los objetivos del área. • Solicitar al Departamento de Tecnologías de la Información y Comunicaciones (DTIC) la atención de incidencias, mantenimiento, actualizaciones o mejoras requeridas por el sistema. • Participar en las pruebas funcionales del Sistema de Informes cuando se implementan nuevas funcionalidades o actualizaciones que impacten la operación del área.
Obligaciones	<ul style="list-style-type: none"> • Utilizar el Sistema de Informes exclusivamente para el desempeño de las funciones institucionales que tiene encomendadas. • Resguardar la confidencialidad de su usuario y contraseña, evitando compartir sus credenciales de acceso con terceras personas. • Cerrar la sesión del sistema al concluir sus actividades o cuando deje desatendido el equipo de cómputo, con el fin de prevenir accesos no autorizados.

	<ul style="list-style-type: none"> • Verificar que la información registrada sea correcta antes de almacenarla o validarla dentro del Sistema de Informes. • Tratar los datos personales contenidos en el sistema conforme a la normativa aplicable en materia de protección de datos personales y a los lineamientos institucionales. • Informar de manera inmediata al DTIC y a la persona responsable del sistema sobre cualquier incidente de seguridad, pérdida de información o acceso no autorizado del que tenga conocimiento. • Utilizar únicamente los equipos y medios autorizados por la institución para acceder al Sistema de Informes.
--	---

2. Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

CIEG Departamento de Tecnologías de la Información y Comunicaciones	
Identificador único	CIEG/SII
Nombre del sistema	Sistema Interno de Informes
Tipo de soporte	Físico y electrónico
Descripción	Base de datos relacional
Características del lugar donde se resguardan los soportes:	El sistema de informes se encuentra en el servidor ubicado en las instalaciones del Departamento de Tecnologías de la Información y Comunicaciones del CIEG. El equipo se encuentra en un área de acceso restringido bajo resguardo institucional con videovigilancia las 24 horas, así como una cerradura de seguridad en donde solo ingresa personal autorizado. El acceso al sistema se controla mediante autenticación por usuario y contraseña, así como medidas de seguridad lógica.

3. Análisis de riesgos

4. Análisis de brecha

5. Plan de trabajo

6. Medidas de seguridad implementadas

6.1. Transferencias de datos personales

CIEG Departamento de Tecnologías de la Información y Comunicaciones	
Identificador único	CIEG/SII
Nombre del sistema	Sistema Interno de Informes
Transferencia de Datos Personales	
Transferencias mediante el traslado de soportes físicos	No Aplica
Transferencias mediante el traslado de soportes electrónicos	No Aplica
Transferencias mediante el traslado sobre redes electrónicas	No Aplica

6.2. Resguardo de sistemas de tratamiento de datos personales con soportes físicos

El servidor donde se aloja el sistema SSI se encuentra en las instalaciones del Departamento de Tecnologías de la Información y Comunicaciones del CIEG, en un site con aire acondicionado ajustado a la temperatura recomendada para la operación óptima de los equipos, este se encuentra bajo acceso restringido únicamente a personal autorizado por medio de personal de vigilancia, así como cámaras que graban las 24 horas y una cerradura de seguridad, con la llave bajo la responsabilidad y resguardo de la persona encargada designada.

Acceso a los soportes físicos del sistema

Nombre: Servando Arturo Jiménez Colín

Cargo: Jefe del Departamento de Tecnologías de la Información y Comunicaciones

Funciones:

- Dirigir y supervisar la operación del Sistema de Informes, asegurando que funcione de manera continua, eficiente y conforme a las necesidades institucionales.
- Supervisar el cumplimiento de las políticas, lineamientos y procedimientos relacionados con el tratamiento y protección de los datos personales contenidos en el sistema.
- Coordinar las actividades de mantenimiento preventivo y correctivo del aplicativo, la infraestructura tecnológica y la base de datos que soportan el Sistema de Informes.
- Autorizar y supervisar la implementación de actualizaciones del sistema, verificando previamente su compatibilidad y minimizando el impacto en la operación institucional.

- Promover la mejora continua del Sistema de Informes mediante la evaluación periódica de su desempeño, disponibilidad, seguridad y cumplimiento de los objetivos institucionales.

Obligaciones:

- Garantizar que el tratamiento de los datos personales realizado mediante el Sistema de Informes se efectúe conforme a la legislación en materia de protección de datos personales y a la normatividad institucional universitaria.
- Asegurar que únicamente el personal autorizado tenga acceso al sistema y a la información contenida en él, conforme a los perfiles y privilegios previamente definidos.
- Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.
- Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente.
- No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales.
- Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente.
- Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales.

6.3. Bitácoras para accesos y operación cotidiana

Los datos que se registran en las bitácoras:

- Únicamente pueden acceder a dichos datos el correspondiente personal autorizado.
- Las bitácoras se almacenan en soporte electrónico. Se pueden realizar acciones como altas, bajas y modificaciones de usuarios, cambios de configuración.
- Las bitácoras generalmente se almacenan en la base de datos del aplicativo instalada en el servidor o equipo que administra el sistema. El tiempo de conservación es de aproximadamente un año o hasta que sean borradas por el mismo sistema o por una persona administradora.
- La integridad de las bitácoras se asegura mediante controles de acceso al aplicativo y a la base de datos, autenticación de usuarios, restricciones de permisos, respaldos periódicos.
- El área responsable de la administración del sistema es el Departamento de Tecnologías de la Información y Comunicaciones de la Información, el cual realiza revisiones mensuales y, en caso de que ocurra un incidente, se hace una revisión extraordinaria.
- El análisis de las bitácoras electrónicas se realiza mediante el módulo de generación de reportes del software.

6.4. Registro de incidentes

El personal que haya notado el incidente, debe dirigirse a la persona responsable de DTIC que determinará la mejor acción necesaria para solucionar la incidencia y atenderla.

6.5. Acceso a las instalaciones

- Seguridad perimetral exterior (las instalaciones del área universitaria): En la entrada principal de edificio de la Torre II de Humanidades se cuenta con acceso controlado, puesto que para poder ingresar al edificio debe permitirse la entrada por personal de vigilancia UNAM, además de contar con videovigilancia las 24 horas en pasillos y demás áreas de las instalaciones. Se lleva un registro de las personas externas detallando el área donde se dirigen, el piso y el funcionario que visita, así como la hora de entrada y de salida.
- Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos): En la entrada principal del CIEG también se cuenta con acceso controlado, ya que para poder ingresar a las oficinas debe permitirse la entrada por personal de vigilancia, además de contar con videovigilancia las 24 horas en pasillos y demás áreas de las instalaciones. Se lleva un registro de las personas externas detallando el nombre, motivo de la visita, hora de entrada y salida, así como identificar a la persona con quien se tiene programada la visita en la institución.

6.6. Actualización de la información contenida en el sistema de tratamiento de datos personales

Para el cambio o actualización de la información debe ser requerido por la persona titular correspondiente o representante de las y los trabajadores de la dependencia a la persona titular del DTIC quien valorará y atenderá la petición siguiendo el protocolo correspondiente.

6.7. Perfiles de usuario y contraseñas

I. Modelo de control de acceso

El Sistema Interno de Informes está basado en roles de usuario, donde se tiene acceso a distintos módulos de acuerdo con sus respectivos privilegios.

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

No se cuenta con un sistema operativo de red.

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

El sistema cuenta con un manejo riguroso de perfiles de usuario y contraseña, así como un cifrado de contraseñas mediante *hash*.

IV. Administración de perfiles de usuario y contraseñas

La persona titular del Departamento de Tecnologías de la Información y Comunicaciones es quien gestiona la administración de los perfiles y realiza el procedimiento correspondiente.

V. Acceso remoto al sistema de tratamiento de datos personales

No se permite el acceso remoto en los equipos de cómputo en los que se encuentra el sistema.

6.8. Procedimiento de respaldo y recuperación de datos

Señalar si realiza respaldos:

- Completos X, diferenciales ____ o incrementales ____
- De forma automática ____ o Manual X
- Periodicidad con que los realiza: ____ mensual ____
- El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: se utiliza un disco duro.
- Cómo y dónde se archivan esos medios: en la unidad de almacenamiento incluida.
- Quién es la persona responsable de realizar estas operaciones (el área universitaria o una tercera persona): los respaldos los realiza completos el sistema automáticamente y lo resguarda la persona responsable de DTIC.

6.9. Plan de contingencia

El Sistema de Informes Interno cuenta con un plan de contingencia cuyo objetivo es garantizar la continuidad de la operación y la recuperación de la información ante incidentes que afecten su disponibilidad. Como parte del proceso de recuperación, se verifica la disponibilidad e integridad de las copias de seguridad más recientes y se identifican los componentes necesarios para restablecer el servicio, incluyendo el sistema operativo, el aplicativo, la base de datos y sus configuraciones. Posteriormente, se realiza la restauración de la información, se verifican las funcionalidades del sistema y se documentan las acciones realizadas para garantizar la correcta recuperación del servicio.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/SII	
Nombre del sistema	Sistema Interno de Informes	
Recurso	Descripción	Control
Bitácoras generadas por el DTIC	Registran las actividades de administración, mantenimiento, actualización, respaldo y atención de incidentes realizadas sobre el Sistema de Informes y la infraestructura que lo soporta.	Las bitácoras son revisadas periódicamente por el personal autorizado del DTIC para verificar el cumplimiento de los procedimientos establecidos, detectar anomalías y documentar las acciones correctivas implementadas.
Bitácoras generadas por el servidor	Se registran los eventos relacionados con la operación del servidor, incluyendo la autenticación de usuarios, acceso al sistema operativo, eventos de seguridad, errores, fallas de hardware y software, así como el funcionamiento de los servicios asociados.	Se realiza una revisión de las bitácoras para identificar eventos inusuales, intentos de acceso no autorizado, fallas del sistema o incidentes que puedan afectar la disponibilidad, integridad o confidencialidad del servicio.
Bitácoras generadas por la base de datos	Se registran las operaciones realizadas sobre la base de datos del sistema, tales como autenticación de usuarios, consultas, inserciones, modificaciones, eliminaciones de información, ejecución de procedimientos y eventos relacionados con la administración de la base de datos.	La revisión se realiza mediante herramientas de administración del gestor de base de datos, con el propósito de verificar la integridad de la información, detectar operaciones inusuales y mantener la trazabilidad de las actividades realizadas sobre los datos personales.

7.2. Procedimiento para la revisión de las medidas de seguridad

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/SII	
Nombre del sistema	Sistema Interno de Informes	
Medida de seguridad	Procedimiento	Responsable
No Aplica	No Aplica	No Aplica

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/SII		
Nombre del sistema	Sistema Interno de Informes		
Medida de seguridad	Procedimiento	Responsable	
No Aplica	No Aplica	No Aplica	

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/SII		
Nombre del sistema	Sistema Interno de Informes		
Medida de seguridad	Procedimiento	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

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/SII		
Nombre del sistema	Sistema Interno de Informes		
Actividad	Descripción	Duración	Cobertura
No Aplica	No Aplica	No Aplica	No Aplica

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/SII		
Nombre del sistema	Sistema Interno de Informes		
Actividad	Descripción	Duración	Cobertura
No Aplica	No Aplica	No Aplica	No Aplica

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/SII		
Nombre del sistema	Sistema Interno de Informes		
Actividad	Descripción	Duración	Cobertura
Análisis de reportes de incidencias de usuarios	Evaluar los reportes de fallas, observaciones y sugerencias recibidas para identificar oportunidades de mejora en el funcionamiento y la usabilidad del Sistema de Informes.	Permanente	Optimización continua del sistema y atención oportuna de incidencias.

Revisión y optimización de mensajes del sistema	Revisar los mensajes de error, advertencia y confirmación para que sean claros, precisos y faciliten para el usuario la usabilidad del sistema.	1 mes	Mejorar la experiencia de las y los usuarios y reducir errores durante la operación.
---	---	-------	--

9.2. Actualización y mantenimiento de equipo de cómputo

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/SII		
Nombre del sistema	Sistema Interno de Informes		
Actividad	Descripción	Duración	Cobertura
Actualizar y reemplazar los equipos que sean necesarios para el funcionamiento del sistema	Mantener el estado de los equipos donde se encuentra el sistema de informes en óptimas condiciones para su desarrollo.	Anual	Garantizar la disponibilidad, continuidad operativa y confiabilidad mediante la sustitución oportuna de equipos que hayan alcanzado el fin de su vida útil o presenten fallas que afecten su funcionamiento.

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/SII	
Nombre del sistema	Sistema Interno de Informes	
Medida de seguridad	Procedimiento	Responsable
Respaldo de la base de datos y del sistema	Se realizan respaldos periódicos de la base de datos, del aplicativo y de los archivos de configuración del Sistema de Informes. Las copias de seguridad son verificadas para asegurar su integridad y disponibilidad en caso de requerir la recuperación del sistema.	Servando Arturo Jiménez Colín Jefe del Departamento de TIC

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/SII	
Nombre del sistema	Sistema Interno de Informes	
Medida de seguridad	Procedimiento	Responsable
Borrado seguro de equipos de cómputo	Antes de la baja, sustitución o disposición final de un equipo utilizado para la	Servando Arturo Jiménez Colín Jefe del Departamento de

	operación del Sistema de Informes, se verifica que la información haya sido respaldada, posteriormente, se realiza el borrado seguro de los dispositivos de almacenamiento mediante herramientas que impiden la recuperación de la información y se documenta el procedimiento efectuado.	TIC
Borrado seguro de respaldos y medios de almacenamiento	Cuando los respaldos o medios de almacenamiento dejan de ser necesarios o concluye el periodo de conservación establecido, se realiza su eliminación segura mediante procedimientos que imposibilitan la recuperación de la información, en el caso de disposición física de los medios, ésta se efectúa conforme a los procedimientos institucionales aplicables.	Servando Arturo Jiménez Colín Jefe del Departamento de TIC

10. Procedimiento para la cancelación de un Sistema de Tratamiento de datos personales

El sistema únicamente será cancelado cuando deje de ser necesario para el cumplimiento de su finalidad, una vez que fue autorizada la cancelación del sistema este será bloqueado y se identificarán los datos personales de tal forma que el acceso a ellos este cancelado y solo puedan ser consultados bajo obligaciones legales. Una vez concluido el periodo de bloqueo y siempre que no exista obligación legal de conservar la información, se procederá a la supresión del sistema mediante la eliminación segura de la base de datos, archivos, respaldos y demás componentes que contengan datos personales. La eliminación se realizará utilizando procedimientos de borrado seguro que impidan la recuperación de la información y, cuando corresponda, mediante la destrucción física de los medios de almacenamiento para finalmente documentar las actividades realizadas y la cancelación definitiva del sistema.

SITIO WEB

1. Inventario de Sistemas de Tratamientos de Datos Personales

CIEG Departamento de Tecnologías de la Información y Comunicaciones	
Identificador único	CIEG/WEB (identificador propuesto)
Nombre del sistema	Sitio web institucional del CIEG
Datos personales (sensibles o no) contenidos en el sistema	<p>Identificación: Nombre y apellidos. Incorporar las fotografías de personas si se confirma su publicación o almacenamiento.</p> <p>Personal académico: Grados, instituciones de formación, estancias, trayectoria docente, publicaciones, áreas y líneas de investigación, premios e identificadores de perfiles académicos. No sensibles por sí mismos.</p> <p>Laborales: Cargo, categoría, adscripción, trayectoria profesional y pertenencia a sistemas de reconocimiento académico. Normalmente no sensibles.</p> <p>Contacto laboral: Correo institucional individual y teléfono o extensión asociados a una persona. Los contactos generales de áreas se distinguen de los contactos individualizados.</p> <p>Sensibles: Información explícita sobre identidad de género presente en determinadas semblanzas. Revisar caso por caso otras autodescripciones que puedan revelar aspectos íntimos o generar riesgo de discriminación; no inferir atributos a partir del nombre, imagen o temas de investigación.</p> <p>Registros y navegación: El aviso de privacidad contempla nombre, correo, teléfono, institución, ciudad, entidad federativa, género, fecha de nacimiento e IP. Confirmar qué datos se recaban efectivamente, en qué plataforma, con qué finalidad y quién los resguarda.</p>

Responsable	
Nombre	Servando Arturo Jiménez Colín
Cargo	Jefe del Departamento de Tecnologías de la Información y Comunicaciones
Funciones	<ul style="list-style-type: none"> Estar a cargo de la administración técnica, contenidos, publicación, alojamiento, respaldos, accesos, bitácoras, mantenimiento y atención de incidentes del sitio web, en el ámbito de las atribuciones del DTIC. Administrar la infraestructura y los componentes del sitio que estén bajo competencia del DTIC; coordinar con quien presta el alojamiento cuando corresponda. Gestionar cuentas y permisos previamente

	autorizados, actualizaciones, respaldos, recuperación y registros de administración.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargado/Usuario	
Nombre	Servando Arturo Jiménez Colín
Cargo	Jefe del Departamento de Tecnologías de la Información y Comunicaciones
Funciones	<ul style="list-style-type: none"> • Gestionar, revisar y publicar los contenidos del sitio web. • Verificar exactitud y pertinencia de los datos • Documentar la autorización o fundamento de publicación. • Revisar la necesidad de incluir información sensible. • Solicitar actualizaciones o retiros y establecer los plazos de conservación aplicables.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.

	<ul style="list-style-type: none"> • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
--	---

2. Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

CIEG Departamento de Tecnologías de la Información y Comunicaciones	
Identificador único	CIEG/WEB (identificador propuesto)
Nombre del sistema	Sitio web institucional del CIEG
Tipo de soporte	Electrónico. Confirmar si existen soportes documentales físicos asociados a autorizaciones o solicitudes.
Descripción	<p>El sitio se utiliza en un sistema CRM y se aloja en máquinas virtuales del <i>site</i> principal del CIEG. Permite consultar información institucional y contenidos vinculados a personas identificadas. Queda pendiente documentar las versiones, base de datos, repositorios y servicios externos asociados.</p> <p>Finalidad: Difundir las actividades del CIEG, su directorio y la trayectoria de su personal; facilitar el contacto</p>

	<p>académico e institucional.</p> <p>El inventario incluye los informes institucionales de la sección Informes CIEG y sus anexos y documentos descargables. Contienen datos personales de identificación, académicos y laborales; queda pendiente revisar cada documento para detectar información sensible o estadísticas que permitan identificar indirectamente a personas. Se propone revisar tanto las publicaciones existentes como las futuras y determinar las medidas de protección o versiones públicas correspondientes.</p> <p>Delimitar subdominios, plataformas externas y formularios enlazados; un enlace no demuestra almacenamiento en el sitio principal. Confirmar cuentas, bitácoras, versiones históricas y respaldos. Revisar el identificador del parámetro "rfc" en enlaces a HUMANINDEX y la necesidad de exponerlo.</p>
Características del lugar donde se resguardan los soportes:	<p>El sitio web se aloja en los servidores ubicados en el <i>site</i> principal del CIEG, donde también se resguardan los respaldos. Responsable: Servando Arturo Jiménez Colín, Jefe del DTIC. Por confirmar: componentes y versiones; controles de acceso físico y administrativo remoto; formularios, analítica e integraciones externas.</p>

3. Análisis de riesgos

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

4. Análisis de brecha

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

5. Plan de trabajo

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

The image displays a 4x4 grid of 16 squares, each containing a unique black and white pixelated pattern. The patterns are symmetrical and resemble stylized, abstract shapes or characters. The central squares (rows 2 and 3, columns 2 and 3) feature more complex, interconnected black shapes, while the outer squares (rows 1 and 4, columns 1 and 4) show simpler, more isolated patterns. The overall effect is a symmetrical, abstract composition.

6. Medidas de seguridad implementadas

6.1. Transferencias de datos personales

CIEG Departamento de Tecnologías de la Información y Comunicaciones	
Identificador único	CIEG/WEB (identificador propuesto)
Nombre del sistema	Sitio web institucional del CIEG
Transferencia de Datos Personales	
Transferencias mediante el traslado de soportes físicos	Por confirmar: existencia de transferencias mediante soportes físicos, datos, destinatarios, finalidad y fundamento.
Transferencias mediante el traslado de soportes electrónicos	Por confirmar: existencia de transferencias mediante soportes electrónicos, datos, destinatarios, finalidad y fundamento.
Transferencias mediante el traslado sobre redes electrónicas	El aviso publicado indica que no se realizan transferencias a terceros, salvo las previstas legalmente. Confirmar los flujos mediante soportes físicos, electrónicos y redes; identificar destinatario, finalidad, datos y fundamento. Distinguir la difusión pública, el alojamiento por cuenta del CIEG y las transferencias conforme a su naturaleza jurídica. No marcar "No aplica" sin revisar formularios y servicios externos.

6.2. Resguardo de sistemas de tratamiento de datos personales con soportes físicos

Los servidores, respaldos y documentos de autorización asociados al sitio web se encuentran en el *site* principal del CIEG, bajo la responsabilidad de Servando Arturo Jiménez Colín, jefe del Departamento de Tecnologías de la Información y Comunicaciones. Queda pendiente documentar los controles de acceso físico, las

condiciones ambientales, el registro de ingresos y las personas adicionales con acceso, si las hubiera.

Acceso a los soportes físicos del sistema

Nombre: Servando Arturo Jiménez Colín

Cargo: Jefe del Departamento de Tecnologías de la Información y Comunicaciones

Funciones:

- Administrar los servidores y respaldos del sitio web bajo competencia del DTIC; coordinar el mantenimiento y la recuperación de los componentes afectados.
- Documentar los controles de acceso a los soportes, las personas autorizadas y las condiciones de resguardo; reportar incidentes que comprometan los datos personales.

Obligaciones:

- Resguardar la confidencialidad, integridad y disponibilidad de la información; utilizar los datos exclusivamente para fines autorizados y proteger credenciales y soportes.
- Evitar copias en medios personales y accesos no autorizados; reportar incidentes y conservar evidencia de las operaciones relevantes.

6.3. Bitácoras para accesos y operación cotidiana

Actualmente no se lleva una bitácora formal de las revisiones. Se propone registrar cuenta, fecha y hora, acción y resultado de las operaciones administrativas; limitar el acceso y proteger la integridad de los registros. Responsable: Servando Arturo Jiménez Colín, jefe del DTIC. Queda pendiente documentar los registros automáticos existentes, su ubicación y conservación. No registrar contraseñas ni datos sensibles innecesarios.

6.4. Registro de incidentes

Propuesta: reportar al DTIC; registrar detección, alcance, datos afectados y medidas de contención; preservar evidencia; corregir la causa y recuperar el servicio; escalar a la instancia competente para evaluar las comunicaciones exigibles a titulares y autoridades. Cerrar el registro con responsables, fechas y acciones preventivas. Confirmar canal y personas responsables de escalamiento.

6.5. Acceso a las instalaciones

- Seguridad perimetral exterior: En la entrada principal de edificio de la Torre II de Humanidades se cuenta con acceso controlado, puesto que para poder ingresar al edificio debe permitirse la entrada por personal de vigilancia UNAM, además de contar con videovigilancia las 24 horas en pasillos y demás áreas de las instalaciones. Se lleva un registro de las personas externas detallando

el área donde se dirigen, el piso y el funcionario que visita, así como la hora de entrada y de salida.

- Seguridad perimetral interior: En la entrada principal del CIEG también se cuenta con acceso controlado, ya que para poder ingresar a las oficinas debe permitirse la entrada por personal de vigilancia, además de contar con videovigilancia las 24 horas en pasillos y demás áreas de las instalaciones. Se lleva un registro de las personas externas detallando el nombre, motivo de la visita, hora de entrada y salida, así como identificar a la persona con quien se tiene programada la visita en la institución.

6.6. Actualización de la información contenida en el sistema de tratamiento de datos personales

Propuesta: recibir solicitudes por un canal institucional; verificar identidad y competencia según el trámite; obtener validación del área responsable del contenido; ejecutar el cambio y registrar fecha, autorización y resultado. Revisar el directorio y las semblanzas durante el uso habitual y al recibir solicitudes de actualización. Los derechos ARCO se tramitarán por los canales institucionales de la UNAM.

6.7. Perfiles de usuario y contraseñas

I. Modelo de control de acceso

La administración del sitio se realiza mediante cuentas y permisos de WordPress. Se propone limitar los privilegios a las funciones asignadas y revocar accesos al concluirlos. Por confirmar: padrón de cuentas y denominación de los perfiles técnicos autorizados.

II. Perfiles de usuario y contraseñas en el sistema operativo de red

Por confirmar: sistema operativo, cuentas, privilegios y controles de acceso de los servidores y máquinas virtuales que alojan el sitio web.

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

La administración está a cargo de Servando Arturo Jiménez Colín, jefe del DTIC. El acceso al panel de WordPress requiere nombre de usuario o correo electrónico, contraseña y captura de un código numérico mostrado en pantalla como comprobación frente a accesos automatizados. Este código visual no constituye un segundo factor de autenticación. Queda pendiente documentar los perfiles autorizados y el almacenamiento de contraseñas.

IV. Administración de perfiles de usuario y contraseñas

La administración de cuentas, permisos y publicación de contenidos está a cargo de Servando Arturo Jiménez Colín, jefe del DTIC. Queda pendiente confirmar la existencia de otras cuentas autorizadas.

V. Acceso remoto al sistema de tratamiento de datos personales

Por confirmar: condiciones de acceso remoto al servidor y a la administración del sitio web, así como los controles aplicables. No se acredita una prohibición general de acceso remoto.

6.8. Procedimiento de respaldo y recuperación de datos

Señalar si realiza respaldos:

- Completos ____, diferenciales ____ o incrementales _____. Tipo por confirmar.
- De forma automática __X__ o Manual _____.
- Periodicidad con que los realiza: semanal. Se conservan las copias correspondientes a las últimas dos semanas.
- Tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad: Por confirmar el medio de almacenamiento utilizado.
- Cómo y dónde archivan esos medios: los respaldos de las máquinas virtuales se resguardan en el *site* principal del CIEG; queda pendiente precisar el medio y sus controles de acceso.
- Quién es la persona responsable de realizar estas operaciones (el área universitaria o una tercera persona): el sistema realiza los respaldos automáticamente, bajo la responsabilidad de Servando Arturo Jiménez Colín, jefe del Departamento de Tecnologías de la Información y Comunicaciones.

6.9. Plan de contingencia

Ante un incidente, Servando Arturo Jiménez Colín, jefe del DTIC, coordinará la recuperación. Se propone identificar y contener la afectación; corregir la causa; seleccionar el respaldo íntegro más reciente adecuado entre las copias de las últimas dos semanas; restaurar la máquina virtual o los componentes afectados; comprobar contenidos, accesos y funcionamiento; y documentar el restablecimiento. Se propone realizar una prueba de restauración para validar el procedimiento y determinar el tiempo de recuperación. La restauración puede implicar la pérdida de los cambios posteriores al respaldo seleccionado.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/WEB (identificador propuesto)	
Nombre del sistema	Sitio web institucional del CIEG	
Recurso	Descripción	Control
Herramientas de administración del sitio web	Se utilizan para revisar el sitio durante su operación y atender solicitudes del CRM.	Revisión durante el uso y a solicitud del CRM. Se propone registrar hallazgos y acciones.

7.2. Procedimiento para la revisión de las medidas de seguridad

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/WEB (identificador propuesto)	
Nombre del sistema	Sitio web institucional del CIEG	
Medida de seguridad	Procedimiento	Responsable
Revisión de las medidas de seguridad	Las revisiones se realizan durante el ingreso y uso habitual del sistema y en atención a las solicitudes del CRM, sin un calendario fijo.	Servando Arturo Jiménez Colín, jefe del DTIC.

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/WEB (identificador propuesto)	
Nombre del sistema	Sitio web institucional del CIEG	
Medida de seguridad	Procedimiento	Responsable
Registro de revisiones y resultados	Actualmente no se lleva una bitácora formal de las revisiones y sus resultados. Se propone registrar la fecha, el motivo, los hallazgos y las acciones realizadas.	Servando Arturo Jiménez Colín, Jefe del DTIC.

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/WEB (identificador propuesto)	
Nombre del sistema	Sitio web institucional del CIEG	
Medida de seguridad	Procedimiento	Responsable
Corrección y seguimiento propuestos	Se propone documentar las acciones correctivas derivadas de las revisiones y solicitudes del CRM, incluyendo prioridad,	Servando Arturo Jiménez Colín, jefe del DTIC.

	responsable, fecha de atención y verificación de su solución.	
--	---	--

8. Programa específico de capacitación

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/WEB (identificador propuesto)		
Nombre del sistema	Sitio web institucional del CIEG		
Actividad	Descripción	Duración	Cobertura
Capacitación propuesta	Datos personales y sensibles, permisos, publicación autorizada, credenciales e incidentes. Confirmar calendario y registro de participación.	Sesión inicial de dos horas y actualización anual.	DTIC y personas que validen o publiquen contenidos.

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/WEB (identificador propuesto)		
Nombre del sistema	Sitio web institucional del CIEG		
Actividad	Descripción	Duración	Cobertura
Difusión propuesta	Comunicar el procedimiento editorial y los canales de actualización, ARCO y reporte de incidentes. Conservar evidencia de la comunicación.	Al incorporar usuarios y cuando cambien los procedimientos.	Personas usuarias involucradas en los contenidos.

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/WEB (identificador propuesto)		
Nombre del sistema	Sitio web institucional del CIEG		
Actividad	Descripción	Duración	Cobertura

Actualización y mantenimiento	Las revisiones se realizan durante el uso del sistema y a solicitud del CRM. Como mejora, se propone documentar los cambios y su autorización, probarlos antes de su publicación y prever su reversión; atender vulnerabilidades según su gravedad.	Revisiones durante el uso y a solicitud del CRM; duración de cambios por definir.	Sitio web y componentes bajo competencia del DTIC.
-------------------------------	---	---	--

9.2. Actualización y mantenimiento de equipo de cómputo

CIEG Departamento de Tecnologías de la Información y Comunicaciones			
Identificador único	CIEG/WEB (identificador propuesto)		
Nombre del sistema	Sitio web institucional del CIEG		
Actividad	Descripción	Duración	Cobertura
Revisión de equipo de cómputo	Revisar anualmente capacidad, soporte y continuidad de los equipos propios utilizados; coordinar con el proveedor cuando la infraestructura no sea del CIEG. Registrar necesidades y decisiones de mantenimiento.	Revisión anual propuesta; duración por definir.	Equipos propios utilizados y coordinación con proveedor cuando corresponda.

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/WEB (identificador propuesto)	
Nombre del sistema	Sitio web institucional del CIEG	
Medida de seguridad	Procedimiento	Responsable
Conservación y respaldos	Se genera una copia automática semanal de las máquinas virtuales y se conservan las copias de las últimas dos semanas en el	Servando Arturo Jiménez Colín, jefe del DTIC.

	<p>site principal del CIEG. Los plazos de conservación de contenidos, solicitudes, autorizaciones y bitácoras se definirán por separado conforme a las obligaciones aplicables. La baja pública de un dato no equivale a eliminar todas sus copias.</p>	
--	---	--

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

CIEG Departamento de Tecnologías de la Información y Comunicaciones		
Identificador único	CIEG/WEB (identificador propuesto)	
Nombre del sistema	Sitio web institucional del CIEG	
Medida de seguridad	Procedimiento	Responsable
Borrado seguro y disposición final propuestos	Al concluir los plazos, verificar que no exista obligación de conservación; eliminar datos con métodos adecuados al medio; documentar alcance, fecha y responsable. En servicios externos, solicitar evidencia de eliminación según los acuerdos aplicables. Evitar prometer eliminación inmediata de todas las copias sin verificar su ciclo de retención.	Servando Arturo Jiménez Colín, jefe del DTIC.

10. Procedimiento para la cancelación de un Sistema de Tratamiento de datos personales

Propuesta: La instancia competente autorizará la cancelación e indicará motivo y fecha. Se hará un inventario de datos, soportes, servicios y dependencias; se definirán destino y plazos de conservación o bloqueo conforme a las obligaciones aplicables. Durante el bloqueo, se restringirá el acceso a las finalidades legalmente permitidas. Concluidos los plazos y verificada la ausencia de impedimentos, se suprimen de forma segura los datos y componentes correspondientes, incluidas las copias bajo control institucional. Se revocarán cuentas y accesos, se tramitará la baja de servicios y se conservará constancia de autorización, ejecución y verificación. Ejecución técnica: Servando Arturo Jiménez Colín, jefe del DTIC. Confirmar técnicas y plazos antes de la cancelación.

SISTEMAS TRANSVERSALES

SISTEMA INTEGRAL DE PERSONAL

CIEG Dirección	
Identificador único	SIP
Nombre del sistema	Sistema Integral de Personal
Datos personales (sensibles o no) contenidos en el sistema	Nombre, CURP, RFC, domicilio, condición migratoria, teléfono y número de empleado del personal de confianza, académico y funcionariado.

Encargada/Usuaría	
Nombre	Amneris Chaparro Martínez
Cargo	Directora
Funciones	<ul style="list-style-type: none"> Firmar contratos del personal de confianza, académico y funcionariado.
Obligaciones	<ul style="list-style-type: none"> Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría	
Nombre	Marlene Carolina Pérez Limón
Cargo	Secretaría Administrativa
Funciones	<ul style="list-style-type: none"> Autorización de contratos, adendas, notificaciones, trámites o servicios y ropa de trabajo.

Obligaciones	<ul style="list-style-type: none"> • Validación de Información. • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
---------------------	--

Encargada/Usuaría	
Nombre	Wendy Mortera Ruenes
Cargo	Jefa del Departamento de Personal
Funciones	<ul style="list-style-type: none"> • Realizar movimientos de contratación, bajas, licencias, prestaciones, servicios, certificaciones, ropa de trabajo, transferencia de plazas, gestión de pagos
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente.

	<ul style="list-style-type: none">• Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales.• Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
--	--

MÓDULO DE SERVICIOS PROFESIONALES

CIEG Secretaría Administrativa	
Identificador único	HONORARIOS
Nombre del sistema	Módulo de Servicios Profesionales
Datos personales (sensibles o no) contenidos en el sistema	Nombre, domicilio, teléfono, CURP, RFC,

Encargada/Usuaría	
Nombre	Marlene Carolina Pérez Limón
Cargo	Secretaría Administrativa
Funciones	<ul style="list-style-type: none"> Revisión de contratos Validación y actualización de Información.
Obligaciones	<ul style="list-style-type: none"> Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría	
Nombre	Wendy Mortera Ruenes
Cargo	Jefa del Departamento de Personal
Funciones	<ul style="list-style-type: none"> Registro de personal para generar contrato por servicios profesionales
Obligaciones	<ul style="list-style-type: none"> Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones.

	<ul style="list-style-type: none"> • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
--	--

NÓMINA INSTITUCIONAL UNAM

CIEG Departamento de Personal	
Identificador único	NÓMINA
Nombre del sistema	Nómina institucional UNAM
Datos personales (sensibles o no) contenidos en el sistema	Número de trabajador, RFC

Encargada/Usuaría	
Nombre	Wendy Mortera Ruenes
Cargo	Jefa del Departamento de Personal
Funciones	<ul style="list-style-type: none"> • Dar de alta al personal para pago de nómina • Suspender pago del personal
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

ESTÍMULOS UNAM

CIEG Departamento de Personal	
Identificador único	Estímulos
Nombre del sistema	Estímulos UNAM
Datos personales (sensibles o no) contenidos en el sistema	Número de trabajador, RFC

Encargada/Usuaría	
Nombre	Wendy Mortera Ruenes
Cargo	Jefa del Departamento de Personal
Funciones	<ul style="list-style-type: none"> Registro del personal al programa de estímulos Registro de incidencias del personal Registro de evaluaciones para envío a la Dirección General de Personal (DGPe)
Obligaciones	<ul style="list-style-type: none"> Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría	
Nombre	Ixchel Uribe Alcántara
Cargo	Jefa del Departamento de Asuntos del Personal Académico
Funciones	<ul style="list-style-type: none"> Hacer el registro de las personas integrantes de la Comisión Evaluadora PRIDE (con su RFC y correo electrónico).

	<ul style="list-style-type: none"> • Dar seguimiento al registro de solicitudes para ingreso, reingreso, renovación o exención del Programa de Primas al Desempeño del Personal Académico hasta la deliberación de la Comisión Evaluadora PRIDE y posterior ratificación, o en su caso presentación y resolución recursos de revisión. • Dar seguimiento al Programa de Estímulos por Equivalencia (PEE) y al Programa de Estímulos de iniciación de la Carrera Académica para Personal de Tiempo Completo (PEI). • Realizar lay carga de la aprobación de informes y programas de actividades anuales.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

TRÁMITE DE PAGO POR OTROS SERVICIOS DEL PERSONAL UNAM

CIEG Departamento de Personal	
Identificador único	PAGOS SERVICIOS UNAM
Nombre del sistema	Trámite de Pago por Otros Servicios del Personal UNAM
Datos personales (sensibles o no) contenidos en el sistema	Número de trabajador, RFC, CURP

Encargada/Usuaria	
Nombre	Wendy Mortera Ruenes
Cargo	Jefa del Departamento de Personal
Funciones	<ul style="list-style-type: none"> Registro del personal que laboró cláusula 15, para proceder al pago.
Obligaciones	<ul style="list-style-type: none"> Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

SISTEMA DE ADMINISTRACIÓN INSTITUCIONAL

CIEG Dirección	
Identificador único	SAI
Nombre del sistema	Sistema de Administración Institucional
Datos personales (sensibles o no) contenidos en el sistema	Nombre o razón social, CURP, RFC, domicilio y correo electrónico de personas prestadoras de servicios profesionales, personas proveedoras y personal de confianza, académico y funcionariado. Nombre de las personas responsables de los diferentes departamentos del CIEG.

Encargada/Usuaría	
Nombre	Amneris Chaparro Martínez
Cargo	Directora
Funciones	<ul style="list-style-type: none"> Firmar pagos y honorarios de personas prestadoras de servicios profesionales, personas proveedoras y personal de confianza, académico y funcionariado.
Obligaciones	<ul style="list-style-type: none"> Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría	
Nombre	Marlene Carolina Pérez Limón
Cargo	Secretaría Administrativa
Funciones	<ul style="list-style-type: none"> Autorización de compra de servicios, productos o materiales, así como bienes muebles.

Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
---------------------	--

Encargada/Usaria	
Nombre	Gabriela García Veramendi
Cargo	Jefa del departamento de Bienes y Suministros
Funciones	<ul style="list-style-type: none"> • Realizar adquisiciones de bienes y servicios en apego a las disposiciones que establezca la UNAM.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales.

	<ul style="list-style-type: none"> • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
--	--

Encargada/Usuaría

Nombre	Nancy Ordoñez Plata
Cargo	Jefa del Departamento de Presupuesto
Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargado/Usuario

Nombre	Roberto Andrés Bustamante López
Cargo	Asistente de procesos del Departamento de Presupuesto
Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.

Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
---------------------	--

Encargada/Usuaría	
Nombre	Wendy Mortera Ruenes
Cargo	Jefa del Departamento de Personal
Funciones	<ul style="list-style-type: none"> • Registrar al personal prestador de servicios profesionales para su pago
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente.

	<ul style="list-style-type: none"> • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
--	---

Encargado/Usuario	
Nombre	Juan Carlos Mendoza Hernández
Cargo	Jefe de Servicios Generales
Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría	
Nombre	Lucía Núñez Rebolledo
Cargo	Secretaría Académica

Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría	
Nombre	Araceli Cervera Guzmán
Cargo	Asistente de procesos de la Secretaría Académica
Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.

Obligaciones

- Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones.
- Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables.
- Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.
- Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente.
- No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales.
- Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente.
- Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales.
- Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría

Nombre	Elizabeth Zúñiga Sandoval
Cargo	Jefa del Departamento de Publicaciones
Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.

Obligaciones

- Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones.
- Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables.
- Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.
- Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente.
- No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales.
- Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente.
- Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales.
- Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargado/Usuario

Nombre	Ubaldo Araujo Esquivel
Cargo	Asistente de procesos del Departamento de Publicaciones
Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.

Obligaciones

- Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones.
- Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables.
- Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.
- Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente.
- No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales.
- Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente.
- Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales.
- Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría

Nombre	Hortensia Manuela Moreno Esparza
Cargo	Directora de Debate Feminista
Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.

Obligaciones

- Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones.
- Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables.
- Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.
- Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente.
- No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales.
- Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente.
- Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales.
- Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría

Nombre	Paola Gabriela Ortega Garay
Cargo	Técnica Académica, Debate Feminista
Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.

Obligaciones

- Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones.
- Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables.
- Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.
- Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente.
- No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales.
- Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente.
- Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales.
- Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargadx/Usuarix

Nombre	César Torres Cruz
Cargo	Investigadorx
Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.

Obligaciones

- Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones.
- Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables.
- Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.
- Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente.
- No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales.
- Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente.
- Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales.
- Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría

Nombre	Lucía Gabriela Ciccía
Cargo	Investigadora
Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.

Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
---------------------	--

Encargada/Usuaría	
Nombre	Luz Adriana Arreola Paz
Cargo	Secretaria Técnica
Funciones	<ul style="list-style-type: none"> • Ingresar cotizaciones de proveedores.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales.

	<ul style="list-style-type: none"> • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
--	--

Encargada/Usuaría	
Nombre	Alba Jiménez Escobar
Cargo	Coordinadora Biblioteca "Rosario Castellanos"
Funciones	<ul style="list-style-type: none"> • Ingresar órdenes de compra y cotizaciones de proveedores.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría	
Nombre	Brenda Margarita Macías Sánchez
Cargo	Jefa del Departamento de Difusión y Comunicación Social
Funciones	<ul style="list-style-type: none"> • Ingresar cotizaciones de proveedores.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.

	<ul style="list-style-type: none"> • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
--	--

Encargado/Usuario	
Nombre	Servando Arturo Jiménez Colín
Cargo	Jefe del Departamento de Tecnologías de la Información y Comunicaciones
Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría	
Nombre	Laura Patricia Bejarano Espinosa
Cargo	Secretaría de Planeación y Vinculación
Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría	
Nombre	Lilián Adelina Limón Rosas
Cargo	Asistente de la Secretaría de Planeación y Vinculación
Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.

Obligaciones

- Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones.
- Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables.
- Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.
- Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente.
- No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales.
- Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente.
- Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales.
- Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría

Nombre	Gabriela Sánchez Flores
Cargo	Jefa del Área de Planeación
Funciones	<ul style="list-style-type: none"> • Atender las solicitudes de compras, reembolsos, servicios profesionales, boletos de avión, viáticos, gastos de intercambio y mensajería. • Dar seguimiento a las solicitudes de pago.

Obligaciones

- Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones.
- Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables.
- Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.
- Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente.
- No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales.
- Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente.
- Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales.
- Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

APLICACIONES DGPO

CIEG Secretaría Administrativa	
Identificador único	App DGPO
Nombre del sistema	Aplicaciones DGPO
Datos personales (sensibles o no) contenidos en el sistema	Nombre, CURP, RFC, número de trabajador, sueldo

Encargada/Usuaría	
Nombre	Marlene Carolina Pérez Limón
Cargo	Secretaria Administrativa
Funciones	<ul style="list-style-type: none"> • Revisión de plantilla • Validación y actualización de información • Autorización de movimientos
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría	
Nombre	Wendy Mortera Ruenes
Cargo	Jefa del Departamento de Personal
Funciones	<ul style="list-style-type: none"> • Conciliación de Plantilla • Recepción de suficiencia presupuestal para ocupar plazas académicas, de confianza y funcionariado

Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
---------------------	--

Encargada/Usaria	
Nombre	Laura Patricia Bejarano Espinosa
Cargo	Secretaria de Planeación y Vinculación
Funciones	<ul style="list-style-type: none"> • Coordinar la elaboración del Anteproyecto de Presupuesto Anual, asegurando que se integre conforme a los lineamientos, plazos y disposiciones aplicables, en congruencia con los objetivos y metas institucionales. • Revisar y autorizar el registro de los reportes trimestrales de los programas presupuestales en los que participa la dependencia, verificando la veracidad, oportunidad y consistencia de la información.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.

	<ul style="list-style-type: none"> • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
--	--

Encargada/Usaria	
Nombre	Gabriela Sánchez Flores
Cargo	Jefa del Área de Planeación
Funciones	<ul style="list-style-type: none"> • Integrar el Anteproyecto de Presupuesto Anual, recopilando y concentrando la información proporcionada por las áreas correspondientes, conforme a los lineamientos y plazos establecidos. • Registrar la Matriz de Indicadores para Resultados (MIR), capturando la información en el sistema institucional, SIISEPRO, de acuerdo con las disposiciones aplicables. • Integrar y registrar los reportes trimestrales de los programas presupuestales en los que participa la dependencia, a través del Módulo de Programación del SIISEPRO, asegurando la oportunidad y consistencia de la información.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente.

	<ul style="list-style-type: none"> • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
--	---

SISTEMA INTEGRAL DE ADMINISTRACIÓN FINANCIERA

CIEG Departamento de Presupuesto	
Identificador único	SIAF
Nombre del sistema	Sistema Integral de Administración Financiera
Datos personales (sensibles o no) contenidos en el sistema	RFC, nombre, razón social, datos bancarios y domicilio

Encargada/Usuaría	
Nombre	Nancy Ordoñez Plata
Cargo	Jefa del Departamento de Presupuesto
Funciones	<ul style="list-style-type: none"> • Dar de alta a proveedores para el registro de los egresos. • Registrar los egresos por proveedor, concepto y partida de gasto. • Generar los formatos administrativos necesarios para solicitar a la Unidad de Proceso Administrativo se realice el pago a los proveedores.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

SISTEMA INTEGRAL DE CONTROL PATRIMONIAL

CIEG Departamento de Bienes y Suministros	
Identificador único	SICOP
Nombre del sistema	Sistema Integral de Control Patrimonial
Datos personales (sensibles o no) contenidos en el sistema	Nombres de responsables del sistema ante la Dirección General del Patrimonio Universitario

Encargada/Usuaría	
Nombre	Gabriela García Veramendi
Cargo	Jefa del Departamento de Bienes y Suministros
Funciones	<ul style="list-style-type: none"> • Altas, bajas y transferencias de bienes cuyo monto es susceptible de inventariarse ante la Dirección General del Patrimonio Universitario con el fin de incorporarlos al registro y control del activo fijo, conforme a la normatividad aplicable.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

PORTAL PATRONATO

CIEG Departamento de Personal	
Identificador único	PATRONATO
Nombre del sistema	Portal Patronato
Datos personales (sensibles o no) contenidos en el sistema	Nombre, CURP, RFC, domicilio, condición migratoria, teléfono, estado de cuenta

Encargada/Usuaría	
Nombre	Wendy Mortera Ruenes
Cargo	Jefa del Departamento de Personal
Funciones	<ul style="list-style-type: none"> • Dar de alta a las personas que reciben pago por servicios profesionales y asimilados
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

MÓDULO DE FACTURA DIGITAL UNAM

CIEG Departamento de Presupuesto	
Identificador único	FACTURA DIGITAL
Nombre del sistema	Módulo de Factura Digital UNAM
Datos personales (sensibles o no) contenidos en el sistema	RFC, nombre completo o Razón Social, código postal, correo electrónico y Régimen Fiscal.

Encargada/Usuaría	
Nombre	Nancy Ordoñez Plata
Cargo	Jefa del Departamento de Presupuesto
Funciones	<ul style="list-style-type: none"> Emitir y enviar la factura electrónica a clientes, por la compra de un bien o servicio. Emitir y enviar la ficha referenciada por la compra de un bien o servicio. Consultar y descargar facturas, tickets y fichas referenciadas previamente emitidas.
Obligaciones	<ul style="list-style-type: none"> Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

SISTEMA DE EVALUACIÓN DE CONCURSOS DE OPOSICIÓN ABIERTOS

CIEG Secretaría Académica	
Identificador único	e-COA
Nombre del sistema	
Datos personales (sensibles o no) contenidos en el sistema	Datos de identificación de las personas aspirantes y concursantes, así como de las personas integrantes de la Comisión Dictaminadora. Datos laborales y académicos de las personas aspirantes y concursantes en los concursos de oposición abiertos del CIEG.

Encargada/Usuaría	
Nombre	Lucía Núñez Rebolledo
Cargo	Secretaria Académica
Funciones	<ul style="list-style-type: none"> • Coordinar el registro de las personas integrantes de la Comisión Dictaminadora. • Monitorear el seguimiento de las etapas de los concursos de oposición abiertos del CIEG (registro de la convocatoria, revisión de solicitudes de ingreso, seguimiento de los requisitos cumplidos, carga de oficios de aceptación y no aceptación, registro de fecha para la presentación de pruebas escritas, carga de oficio dirigido al CTH para enviar la deliberación final y solicitud de la ratificación del resultado de cada concurso).
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría	
Nombre	Ixchel Uribe Alcántara
Cargo	Jefa del Departamento de Asuntos del Personal Académico
Funciones	<ul style="list-style-type: none"> • Registrar de las personas integrantes de la Comisión Dictaminadora. • Dar seguimiento a las etapas de los concursos de oposición abiertos del CIEG (registro de la convocatoria, revisión de solicitudes de ingreso, seguimiento de los requisitos cumplidos, carga de oficios de aceptación y no aceptación, registro de fecha para la presentación de pruebas escritas, carga de oficio dirigido al CTH para enviar la deliberación final y solicitud de la ratificación del resultado de cada concurso).
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

SISTEMA DE INFORMES ACADÉMICOS DEL SUBSISTEMA DE HUMANIDADES

CIEG Secretaría Académica	
Identificador único	e-SIAH
Nombre del sistema	Sistema de Informes Académicos del Subsistema de Humanidades
Datos personales (sensibles o no) contenidos en el sistema	Datos de identificación, datos laborales y académicos del personal académico.

Encargada/Usuaría	
Nombre	Lucía Núñez Rebolledo
Cargo	Secretaria Académica
Funciones	<ul style="list-style-type: none"> • Coordinar el seguimiento al registro del plazo para la presentación de informes y programas de actividades de carácter anual del personal académico. • Supervisar el seguimiento al cumplimiento de la solicitud de registro de programas y programas, solicitud de modificaciones y atención a observaciones, así como el registro de aprobación o no aprobación de los informes. • Revisar la solicitud de altas y bajas del personal académico, registro de la huella digital electrónica que concluye el proceso de evaluación de informes y programas en el sistema e-SIAH, una vez que se obtiene la resolución del CTH.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona

	superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
--	--

Encargada/Usuaría	
Nombre	Ixchel Uribe Alcántara
Cargo	Jefa del Departamento de Asuntos del Personal Académico
Funciones	<ul style="list-style-type: none"> • Llevar a cabo el registro del plazo para la presentación de informes y programas de actividades de carácter anual del personal académico. • Dar seguimiento al cumplimiento de la solicitud de registro de programas y programas, solicitud de modificaciones y atención a observaciones, registro de aprobación o no aprobación de los informes. • Realizar la solicitud de altas y bajas del personal académico, registro de la huella digital electrónica que concluye el proceso de evaluación de informes y programas en el sistema e-SIAH, una vez que se obtiene la resolución del CTH.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

SISTEMA DE GESTIÓN ELECTRÓNICA

CIEG Departamento de Asuntos del Personal Académico	
Identificador único	GeDGAPA
Nombre del sistema	Sistema de Gestión Electrónica
Datos personales (sensibles o no) contenidos en el sistema	Nombre, teléfono, correo electrónico, CURP, RFC, nacionalidad del personal académico

Encargada/Usuaría	
Nombre	Ixchel Uribe Alcántara
Cargo	Jefa del Departamento de Asuntos del Personal Académico
Funciones	<ul style="list-style-type: none"> • Registrar el nivel máximo de estudio y carga de constancias de la obtención de grado de licenciatura, especialización, maestría, doctorado del personal académico, así como constancia de la realización de posdoctorado. • Registrar las postulaciones y carga de documentación con datos de identificación, laborales y académicos del personal académico al Premio Universidad Nacional (PUN) y al Reconocimiento Distinción Universidad Nacional para Jóvenes Académicos (RDUNJA).
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría	
Nombre	Ana Rosa Dabin Pia
Cargo	Jefa del Departamento de Formación
Funciones	<ul style="list-style-type: none"> • Registrar los cursos ofertados en el Programa de Actualización y Superación Docente (PASD). • Realizar la reprogramación y cancelación de cursos. • Registrar las calificaciones de las personas inscritas a los cursos.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

SISTEMA INTEGRAL DE ESTÍMULO POR ASISTENCIA AL PERSONAL ACADÉMICO DE LA UNAM

CIEG Departamento de Asuntos del Personal Académico	
Identificador único	SIEPA
Nombre del sistema	Sistema Integral de Estímulo por Asistencia al Personal Académico de la UNAM
Datos personales (sensibles o no) contenidos en el sistema	Datos de identificación, laborales y académicos del personal académico

Encargada/Usuaría	
Nombre	Ixchel Uribe Alcántara
Cargo	Jefa del Departamento de Asuntos del Personal Académico
Funciones	<ul style="list-style-type: none"> • Registrar anualmente al personal académico con derecho o no al estímulo por asistencia.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

SISTEMA DE ELECCIONES DE LA DIRECCIÓN GENERAL DE PERSONAL

CIEG Departamento de Asuntos del Personal Académico	
Identificador único	ELECCIONES UNAM
Nombre del sistema	Sistema de Elecciones de la Dirección General de Personal
Datos personales (sensibles o no) contenidos en el sistema	Datos de identificación, laborales y académicos del personal académico.

Encargada/Usuaría	
Nombre	Amneris Chaparro Martínez
Cargo	Directora
Funciones	<ul style="list-style-type: none"> Coordinar la consulta y verificación del personal elegible o elector en los procesos de elección del CIEG (representantes del personal académico ante el Consejo Universitario, el CAACS, el CAAHA y el Consejo Interno).
Obligaciones	<ul style="list-style-type: none"> Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

Encargada/Usuaría	
Nombre	Ixchel Uribe Alcántara
Cargo	Jefa del Departamento de Asuntos del Personal Académico
Funciones	<ul style="list-style-type: none"> Llevar a cabo la consulta, modificación y verificación del personal elegible o elector en los procesos de

	elección del CIEG (representantes del personal académico ante el Consejo Universitario, el CAACS, el CAAHA y el Consejo Interno).
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

SISTEMA DE GESTIÓN KOHA

CIEG Coordinación de Biblioteca	
Identificador único	KOHA
Nombre del sistema	Sistema de gestión Koha
Datos personales (sensibles o no) contenidos en el sistema	Nombre completo, domicilio particular, teléfonos (fijo y celular), correo electrónico personal e institucional, RFC, fecha de nacimiento, edad, número de cuenta de alumnado, número de trabajador UNAM

Encargada/Usuaría	
Nombre	Alba Jiménez Escobar
Cargo	Coordinadora de la Biblioteca "Rosario Castellanos"
Funciones	<ul style="list-style-type: none"> Almacenar información personal de personas usuarias de la biblioteca para gestionar el préstamo de libros y configurar el nombre de usuario y contraseña para la renovación en línea.
Obligaciones	<ul style="list-style-type: none"> Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

DIRECTORIO UNIVERSITARIO

CIEG Departamento del Departamento de Difusión y Comunicación Social	
Identificador único	Directorio UNAM
Nombre del sistema	Directorio Universitario
Datos personales (sensibles o no) contenidos en el sistema	Número de trabajador, CURP

Encargada/Usuaría	
Nombre	Brenda Margarita Macías Sánchez
Cargo	Jefa del Departamento de Difusión y Comunicación Social
Funciones	<ul style="list-style-type: none"> • Actualizar el directorio del CIEG dentro del Directorio General de la UNAM
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

SISTEMA ÁPEIRON

CIEG Secretaría Académica	
Identificador único	a- SECIHTI
Nombre del sistema	Sistema Ápeiron
Datos personales (sensibles o no) contenidos en el sistema	Datos de identificación, datos laborales y académicos del personal académico

Encargada/Usuaría	
Nombre	Lucía Núñez Rebolledo
Cargo	Secretaria Académica
Funciones	<ul style="list-style-type: none"> Firmar las acreditaciones y generación de informes mensuales y anuales del personal académico.
Obligaciones	<ul style="list-style-type: none"> Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.

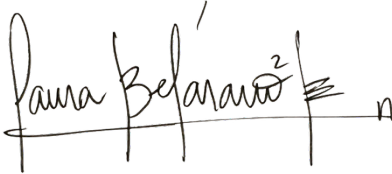
Encargada/Usuaría	
Nombre	Lucía Núñez Rebolledo
Cargo	Secretaria Académica
Funciones	<ul style="list-style-type: none"> Firmar, en suplencia de la Dirección, las acreditaciones y generación de informes mensuales y anuales del personal académico.

Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados. • Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente. • No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales. • Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente. • Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales. • Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
---------------------	--

Encargada/Usuaría	
Nombre	Ixchel Uribe Alcántara
Cargo	Jefa del Departamento de Asuntos del Personal Académico
Funciones	<ul style="list-style-type: none"> • Hacer la carga masiva de información del personal académico, personas becarias posdoctorales que debe ser acreditado en el Sistema Nacional de Investigadoras e Investigadores (SNII) de la Secretaría de Ciencia, Humanidades, Tecnología e Innovación (SECIHTI). • Llevar a cabo las altas y bajas del personal y personas becarias entrantes o salientes de la entidad académica. • Dar seguimiento al proceso de acreditación hasta la generación del informe mensual o anual, según corresponda.
Obligaciones	<ul style="list-style-type: none"> • Resguardar la confidencialidad de los datos personales a los que tenga acceso con motivo de sus funciones. • Realizar el tratamiento de datos personales conforme a la legislación y la normatividad aplicables. • Abstenerse de divulgar, compartir o utilizar los datos personales para fines distintos a los autorizados.

	<ul style="list-style-type: none">• Evitar la modificación, alteración o eliminación de la información almacenada en los sistemas institucionales sin la autorización correspondiente.• No almacenar ni realizar copias de respaldo de datos personales en equipos o dispositivos personales.• Abstenerse de transferir datos personales sin la autorización o fundamento jurídico correspondiente.• Preservar la integridad y disponibilidad de la información resguardada en los sistemas institucionales.• Informar de manera inmediata a la persona superior jerárquica sobre cualquier incidente que comprometa el resguardo, acceso, consulta, uso o disponibilidad de los datos personales.
--	--

APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombres y firmas de quienes revisaron el presente documento
Responsable del desarrollo	Ing. Servando Arturo Jiménez Colín Jefe Del Departamento de Tecnologías de la Información y Comunicaciones Teléfono: 5556222222, ext. 42244 Correo electrónico: dtic@cieg.unam.mx	
Revisó	Mtra. Laura Patricia Bejarano Espinosa Secretaria de Planeación y Vinculación Teléfono: 5556222222, ext. 42162 Correo electrónico: spv@cieg.unam.mx	
Autorizó	Dra. Amneris Chaparro Martínez Directora del Centro de Investigaciones y Estudios de Género Teléfono: 5556222222, ext. 30022 Correo electrónico: direccion@cieg.unam.mx	
Fecha de aprobación	15 de octubre de 2026	
Fecha de actualización	15 de octubre de 2026	