



El presente documento de seguridad describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por la Secretaría Administrativa para garantizar la confidencialidad, integridad y disponibilidad de la información personal contenida en los sistemas de tratamiento de datos personales que utiliza para la realización de sus actividades.

Cabe mencionar que los sistemas informáticos que maneja la Secretaría Administrativa son desarrollos de las direcciones generales adscritas a la misma, por lo que no se tiene ningún desarrollo propio.

Se identifican tres grupos en donde se tratan datos personales:

1. Circuito cerrado de televisión
2. Control de acceso a las instalaciones
3. Actividades de la Unidad Administrativa

En el circuito cerrado de televisión se captan imágenes en cuatro instalaciones, se tiene control de acceso en cuatro instalaciones y en la Unidad Administrativa se manejan datos personales para el desarrollo de las actividades de personal, presupuesto, bienes y suministros y servicios generales. En total doce documentos de seguridad que se relacionan a continuación.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa/Unidad Administrativa/Presupuesto	
Identificador único	SA_UA_P
Nombre del sistema	Presupuesto
Datos personales	Datos de identificación: Nombre (razón social) y RFC.
Responsable	
Nombre	Hugo Enrique Villaseñor Morán
Cargo	Jefe del Departamento de Presupuesto
Funciones	Trámite de pago a proveedores; Elaboración de formas múltiples, reembolsos y viáticos; Elaboración de adecuaciones y recalendarizaciones presupuestales; Realización de la programación presupuestal de los Anteproyectos de Presupuesto; Supervisar el registro, captación y depósito de los ingresos extraordinarios; Elaboración de reportes de los recursos financieros de la dependencia; y Realización de conciliaciones bancarias y presupuestales.
Obligaciones	
Encargados	
Nombre	NO HAY
Usuarios	
Nombre	Sara Gloria Guapillo Ponce
Cargo	Jefe de Área
Funciones	Apoyo en el trámite de pago a proveedores, elaboración de formas múltiples y consulta de información que se genera en el departamento de Presupuesto. * Elaboración y consulta de información mediante usuario y contraseña asignada para el Sistema Integral de Registro Financiero (SIRF), Sistema Integral de Compras (SIC) y Sistema Integral de la Administración Universitaria (SIAU).
Obligaciones	

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

Tipo de soporte	Físico y Electrónico
Descripción	Expedientes
Características del lugar donde se resguardan los soportes	Archivero con llave. Computadora con contraseña

3. ANÁLISIS DE RIESGOS

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

I. TRANSFERENCIAS DE DATOS PERSONALES

TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	Mensajero
Transferencias mediante el traslado de soportes electrónicos:	NO HAY
Transferencias mediante el traslado sobre redes electrónicas:	NO HAY

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

Archiveros con llave.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No existe bitácora.

IV. REGISTRO DE INCIDENTES

- El responsable elabora informe del incidente.
- En caso de robo o extravío, el responsable del sistema da vista al titular de la dependencia para su conocimiento y en el ámbito de sus atribuciones, determine lo conducente.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior

- Se tiene control de acceso con intercomunicador mediante el cual se identifica a la persona que quiere acceder.
- El personal autorizado accede mediante su huella digital.

2. Seguridad perimetral interior

- Computadora con contraseña.

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

La información se actualiza cuando se recaba.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El responsable es el único usuario y modifica su contraseña periódicamente.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El responsable respalda la información en un dispositivo externo que resguarda en una oficina diferente.

IX. PLAN DE CONTINGENCIA

En caso de alguna contingencia se recupera el sistema a través del respaldo. No se cuenta con sitio alternativo.

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

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

Recurso	Descripción	Control
ESET Endpoint Security	Antivirus	Automático

7.2. Procedimiento para la revisión de las medidas de seguridad

Medida de seguridad	Procedimiento	Responsable
Archivero con llave Computadora con contraseña.	Verificar su funcionamiento	Hugo Enrique Villaseñor Morán Diario

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

Medida de seguridad	Resultado de evaluación	Responsable
Archivero con llave Computadora con contraseña.	En funcionamiento	Hugo Enrique Villaseñor Morán Diario

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

Medida de seguridad	Acciones	Responsable
Archivero con llave Computadora con contraseña.	Mantenimiento correctivo Mantenimiento preventivo	Hugo Enrique Villaseñor Morán

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9.2. Actualización y mantenimiento de equipo de cómputo

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Proceso	Descripción	Responsable
Integrar expedientes	Abrir expediente Conjuntar la información Archivar expediente	Hugo Enrique Villaseñor Morán

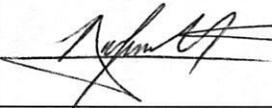
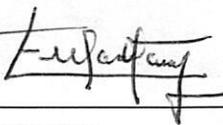
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Proceso	Descripción	Responsable
Borrado seguro	Conforme a la Circular DGTIC/003/2017	Mayra Téllez Hernández
Baja de equipo y/o componentes	Trámite de Baja emitido por la DG del Patrimonio Universitario	Nayeli Hernández Martínez

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

No existe procedimiento de cancelación, el tratamiento de los documentos se realiza conforme al catálogo de disposición documental.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

	Desarrolló	Revisó	Autorizó
Nombre	Hugo Enrique Villaseñor Morán	César Ávalos Hernández	Eduardo Maristany Cáceres
Puesto	Jefe del Departamento de Presupuesto	Jefe de Unidad Administrativa	Responsable de seguridad de datos personales
Teléfono	56221350	5622 1330	5623 0257
Correo Electrónico	h Moran@unam.mx	cavalosh@unam.mx	emaristany@unam.mx
Firma			
Fecha de aprobación	10/08/2022	Fecha de actualización	10/08/2022

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa/Unidad Administrativa/Sistema Integral de Personal	
Identificador único	SA_UA_SIP
Nombre del sistema	Sistema Integral de Personal
Datos personales	Datos Personales en general: Datos de identificación: nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, RFC, CURP, identificación oficial, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de beneficiarios, fotografía; datos laborales: historia curricular, nombramientos, incidencias, capacitación, puesto, referencias laborales, referencias personales; datos académicos: trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos; datos bancarios: Institución bancaria, número de cuenta y CLABE interbancaria. Datos personales sensibles: Incapacidades médicas, uso de lentes oftálmicos, ortopédicos y auditivos.
Responsable	
Nombre	Diana Lilia Cureño Martínez
Cargo	Jefe del Departamento de Personal
Funciones	<ul style="list-style-type: none"> * Realización de movimientos de personal, licencias médicas por gravedad, enfermedad o accidente no profesional. Licencias prejubilatorias y/o prepensionarias. * Elaboración de contratos por Servicios Profesionales y Contratos Individuales de trabajo. Alta, baja por renuncia, defunción o rescisión del personal universitario. * Seguimiento a solicitudes de prestaciones y servicios del personal de la dependencia y subdependencias (constancias, vale de juguetes, cambio de domicilio, apoyo de guardería, reexpedición credenciales). * Trámite de pago de tiempo extraordinario del personal adscrito a la Secretaría Administrativa de la UNAM.
Obligaciones	<ul style="list-style-type: none"> * Resguardo de contraseña asignada para acceso al Sistema Integral de Personal. * Integrar la documentación en el expediente físico del trabajador(a) para resguardar la confidencialidad de este.
Encargados	
Nombre	NO HAY
Usuarios	
Nombre	César Ávalos Hernández
Cargo	Jefe de Unidad Administrativa
Funciones	<ul style="list-style-type: none"> * Consulta de información del personal adscrito a la Secretaría Administrativa de la UNAM. * Autorización mediante firma electrónica de los movimientos y notificaciones realizadas en el SIP.

Obligaciones	* Resguardo de contraseña asignada para acceso al Sistema Integral de Personal.
Nombre	Hugo Villaseñor Moran
Cargo	Jefe del Departamento de Presupuesto
Funciones	* Registro de información en el Sistema Institucional de Registro Financiero (SIRF).
Obligaciones	* Mantener la confidencialidad de la información proporcionada por el Departamento de Personal.
Nombre	Antaar García Ávila
Cargo	Jefe de Departamento
Funciones	* Consulta de información del personal adscrito a la Secretaría Administrativa de la UNAM como apoyo al Jefe de Departamento de Personal. * Registro del pago de tiempo extraordinario del personal adscrito a la Secretaría Administrativa de la UNAM.
Obligaciones	* Resguardo de contraseña asignada para acceso al Sistema Integral de Personal. * Mantener la confidencialidad de la información contenida en el SIP.

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

Tipo de soporte	Físico y Electrónico
Descripción	Expedientes, SIP (usuario)
Características del lugar donde se resguardan los soportes	Archivero con llave. Computadora con contraseña

3. ANÁLISIS DE RIESGOS

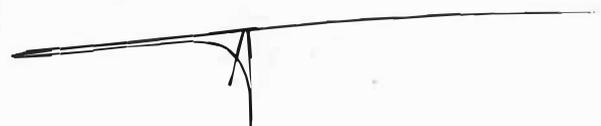
INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO





INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	Mensajero
Transferencias mediante el traslado de soportes electrónicos:	NO HAY
Transferencias mediante el traslado sobre redes electrónicas:	NO HAY

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

Archiveros con llave.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No existe bitácora.

IV. REGISTRO DE INCIDENTES

- El responsable elabora informe del incidente.
- En caso de robo o extravío, el responsable del sistema da vista al titular de la dependencia para su conocimiento y en el ámbito de sus atribuciones, determine lo conducente.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior

- Se tiene control de acceso con intercomunicador mediante el cual se identifica a la persona que quiere acceder.
- El personal autorizado accede mediante su huella digital.

2. Seguridad perimetral interior

- Computadora con contraseña.

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

El responsable es usuario del SIP.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El responsable es usuario del SIP.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El responsable es usuario del SIP.

IX. PLAN DE CONTINGENCIA

El responsable es usuario del SIP.

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

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

Recurso	Descripción	Control
ESET Endpoint Security	Antivirus	Automático

7.2. Procedimiento para la revisión de las medidas de seguridad

Medida de seguridad	Procedimiento	Responsable
Archivero con llave Computadora con contraseña.	Verificar su funcionamiento	Diana Lilia Cureño Martínez Diario

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

Medida de seguridad	Resultado de evaluación	Responsable
Archivero con llave Computadora con contraseña.	En funcionamiento	Diana Lilia Cureño Martínez Diario

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

Medida de seguridad	Acciones	Responsable
Archivero con llave Computadora con contraseña.	Mantenimiento correctivo Mantenimiento preventivo	Diana Lilia Cureño Martínez

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9.2. Actualización y mantenimiento de equipo de cómputo

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Proceso	Descripción	Responsable
Integrar expedientes	Abrir expediente Conjuntar la información Archivar expediente	Diana Lilia Cureño Martínez

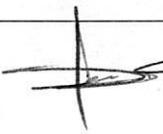
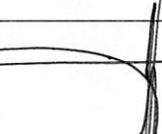
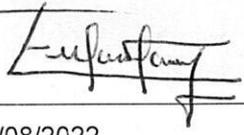
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Proceso	Descripción	Responsable
Borrado seguro	Conforme a la Circular DGTIC/003/2017	Mayra Téllez Hernández
Baja de equipo y/o componentes	Trámite de Baja emitido por la DG del Patrimonio Universitario	Nayeli Hernández Martínez

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

No existe procedimiento de cancelación, el tratamiento de los documentos se realiza conforme al catálogo de disposición documental.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

	Desarrolló	Revisó	Autorizó
Nombre	Diana Lilia Cureño Martínez	César Ávalos Hernández	Eduardo Maristany Cáceres
Puesto	Jefa del Departamento de Personal	Jefe de Unidad Administrativa	Responsable de seguridad de datos personales
Teléfono	555622 1355	555622 1330	555623 0257
Correo Electrónico	dcureno@unam.mx	cavalosh@unam.mx	emaristany@unam.mx
Firma			
Fecha de aprobación	10/08/2022	Fecha de actualización	10/08/2022

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa/Unidad Administrativa/Bienes y Suministros	
Identificador único	SA_UA_BS
Nombre del sistema	Bienes y Suministros
Datos personales	Nombre, teléfono, celular, identificación (INE, pasaporte, cedula fiscal, cartilla), comprobante de domicilio, cedula fiscal, RFC, dirección.
Responsable	
Nombre	Elizabeth Nayeli Hernández Martínez
Cargo	Jefa del Departamento de Bienes y Suministros
Funciones	<ol style="list-style-type: none"> 1. Elaborar contratos de compraventa: <ul style="list-style-type: none"> • Solicitar información y documentos necesarios para elaborar el contrato. • Elaborar el contrato de compra. • Recabar firmas del contrato. • Enviar a depósito y registro el contrato a DGLU. 2. Realizar compras en el SIC: <ul style="list-style-type: none"> • Registrar cada compra en el SIC. • Realizar cotizaciones. • Recibir y revisar producto de proveedores. • Entregar los bienes los usuarios. 3. Registro y elaboración del vale de almacén: <ul style="list-style-type: none"> • Registro en el sistema administrativo integral de la UNAM de presupuesto para registrar las salidas del almacén de bienes de uso recurrente. • Imprimir y pasar a firma los vales de almacén, a cada uno de los usuarios
Obligaciones	<ol style="list-style-type: none"> 1. Elaborar contratos de compraventa, enviar a depósito y registro el contrato de compra cuando esta sea mayor de 2000 salarios. 2. Realizar las compras solicitadas por medio del SIC de los usuarios de la secretaria administrativa. 3. Realizar el registro de salidas de bienes recurrentes en el sistema de presupuesto
Encargados	
Nombre	NO HAY
Usuarios	
Nombre	César Ávalos Hernández
Cargo	Jefe de Unidad Administrativa
Funciones	Supervisar y firmar los contratos, compras y vales de almacén.
Obligaciones	Firmar el contrato y oficio de envió a DGLU, autoriza y firma la compra de bienes de uso recurrente y los vales de almacén.
Nombre	Hugo Villaseñor Moran
Cargo	Jefe del Departamento de Presupuesto
Funciones	Dar suficiencia presupuestal y asignar códigos presupuestales a cada uno de los artículos a comprar.
Obligaciones	Autorizar la compra en base a la suficiencia presupuestal que se tenga para cada partida.

Handwritten signature and initials in the bottom right corner of the page.

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

Tipo de soporte	Físico y Electrónico
Descripción	Expedientes, SIC (usuario)
Características del lugar donde se resguardan los soportes	Archivero con llave. Computadora con contraseña.

3. ANÁLISIS DE RIESGOS

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

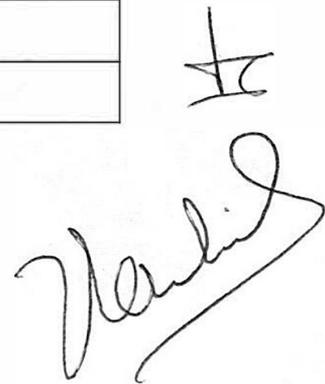
6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	Mensajero
Transferencias mediante el traslado de soportes electrónicos:	NO HAY
Transferencias mediante el traslado sobre redes electrónicas:	NO HAY

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

Archiveros con llave.



III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No existe bitácora.

IV. REGISTRO DE INCIDENTES

- El responsable elabora informe del incidente.
- En caso de robo o extravío, el responsable del sistema da vista al titular de la dependencia para su conocimiento y en el ámbito de sus atribuciones, determine lo conducente.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior

- Se tiene control de acceso con intercomunicador mediante el cual se identifica a la persona que quiere acceder.
- El personal autorizado accede mediante su huella digital.

2. Seguridad perimetral interior

- Computadora con contraseña.

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

El responsable es usuario del SIC.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El responsable es usuario del SIC.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El responsable es usuario del SIC.

IX. PLAN DE CONTINGENCIA

El responsable es usuario del SIC.

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

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

Recurso	Descripción	Control
ESET Endpoint Security	Antivirus	Automático

7.2. Procedimiento para la revisión de las medidas de seguridad

Medida de seguridad	Procedimiento	Responsable
Archivero con llave Computadora con contraseña.	Verificar su funcionamiento	Elizabeth Nayeli Hernández Martínez Diario

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

Medida de seguridad	Resultado de evaluación	Responsable
Archivero con llave Computadora con contraseña.	En funcionamiento	Elizabeth Nayeli Hernández Martínez Diario

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

Medida de seguridad	Acciones	Responsable
Archivero con llave Computadora con contraseña.	Mantenimiento correctivo Mantenimiento preventivo	Elizabeth Nayeli Hernández Martínez

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

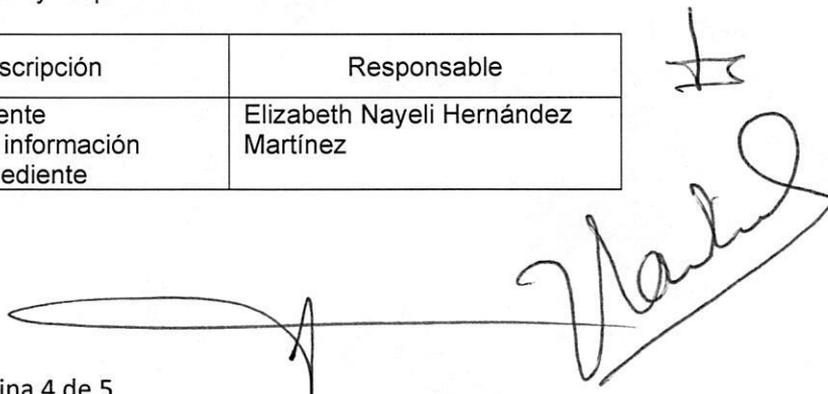
Actividad	Descripción	Duración	Cobertura
NINGUNA			

9.2. Actualización y mantenimiento de equipo de cómputo

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Proceso	Descripción	Responsable
Integrar expedientes	Abrir expediente Conjuntar la información Archivar expediente	Elizabeth Nayeli Hernández Martínez

Handwritten signature and initials in black ink, located at the bottom right of the page. The signature appears to be 'Elizabeth Nayeli Hernández Martínez' and the initials are 'E.N.H.M.'.

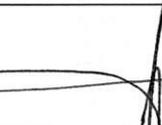
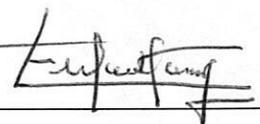
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Proceso	Descripción	Responsable
Borrado seguro	Conforme a la Circular DGTIC/003/2017	Mayra Téllez Hernández
Baja de equipo y/o componentes	Trámite de Baja emitido por la DG del Patrimonio Universitario	Elizabeth Nayeli Hernández Martínez

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

No existe procedimiento de cancelación, el tratamiento de los documentos se realiza conforme al catálogo de disposición documental.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

	Desarrolló	Revisó	Autorizó
Nombre	Elizabeth Nayeli Hernández Martínez	César Ávalos Hernández	Eduardo Maristany Cáceres
Puesto	Jefa del Departamento de Bienes y Suministros	Jefe de Unidad Administrativa	Responsable de seguridad de datos personales
Teléfono	56221339	5622 1330	5623 0257
Correo Electrónico	nayelim@unam.mx	cavalosh@unam.mx	emaristany@unam.mx
Firma			
Fecha de aprobación	10/08/2022	Fecha de actualización	10/08/2022



1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa/Unidad Administrativa/Servicios Generales	
Identificador único	SA_UA_SG
Nombre del sistema	Servicios Generales
Datos personales	RFC, nombre, teléfono, dirección, correo, acta constitutiva, comprobante de domicilio, firma.
Responsable	
Nombre	Jorge Chaires García
Cargo	Jefe del Departamento de Servicios Generales
Funciones	Resguardar la información de Datos Personales de Proveedores de Servicio.
Obligaciones	Mantener el control y resguardo de documentos físicos en el área de servicios generales
Encargados	
Nombre	NO HAY
Usuarios	
Nombre	NO HAY

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

Tipo de soporte	Físico y Electrónico
Descripción	Expedientes
Características del lugar donde se resguardan los soportes	Archivero con llave. Computadora con contraseña

3. ANÁLISIS DE RIESGOS

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	Mensajero
Transferencias mediante el traslado de soportes electrónicos:	NO HAY
Transferencias mediante el traslado sobre redes electrónicas:	NO HAY

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

Archiveros con llave.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No existe bitácora.

IV. REGISTRO DE INCIDENTES

- El responsable elabora informe del incidente.
- En caso de robo o extravío, el responsable del sistema da vista al titular de la dependencia para su conocimiento y en el ámbito de sus atribuciones, determine lo conducente.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior

- Se tiene control de acceso con intercomunicador mediante el cual se identifica a la persona que quiere acceder.
- El personal autorizado accede mediante su huella digital.

2. Seguridad perimetral interior

- Computadora con contraseña.

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

La información se actualiza cuando se recaba.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El responsable es el único usuario y modifica su contraseña periódicamente.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

El responsable respalda la información en un dispositivo externo que resguarda en una oficina diferente.

IX. PLAN DE CONTINGENCIA

En caso de alguna contingencia se recupera el sistema a través del respaldo.
No se cuenta con sitio alternativo.

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

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

Recurso	Descripción	Control
ESET Endpoint Security	Antivirus	Automático

7.2. Procedimiento para la revisión de las medidas de seguridad

Medida de seguridad	Procedimiento	Responsable
Archivero con llave Computadora con contraseña.	Verificar su funcionamiento	Jorge Chaires García Diario

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

Medida de seguridad	Resultado de evaluación	Responsable
Archivero con llave Computadora con contraseña.	En funcionamiento	Jorge Chaires García Diario

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

Medida de seguridad	Acciones	Responsable
Archivero con llave Computadora con contraseña.	Mantenimiento correctivo Mantenimiento preventivo	Jorge Chaires García

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9.2. Actualización y mantenimiento de equipo de cómputo

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Proceso	Descripción	Responsable
Integrar expedientes	Abrir expediente Conjuntar la información Archivar expediente	Jorge Chaires García

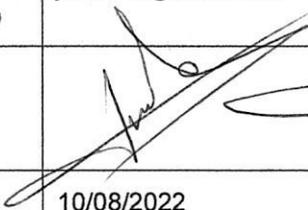
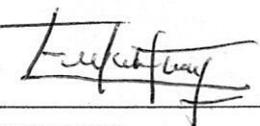
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Proceso	Descripción	Responsable
Borrado seguro	Conforme a la Circular DGTIC/003/2017	Mayra Téllez Hernández
Baja de equipo y/o componentes	Trámite de Baja emitido por la DG del Patrimonio Universitario	Nayeli Hernández Martínez

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

No existe procedimiento de cancelación, el tratamiento de los documentos se realiza conforme al catálogo de disposición documental.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

	Desarrolló	Revisó	Autorizó
Nombre	Jorge Chaires García	César Ávalos Hernández	Eduardo Maristany Cáceres
Puesto	Jefe del Departamento de Servicios Generales	Jefe de Unidad Administrativa	Responsable de seguridad de datos personales
Teléfono	56221342	5622 1330	5623 0257
Correo Electrónico	jchaires@unam.mx	cavalosh@unam.mx	emaristany@unam.mx
Firma			
Fecha de aprobación	10/08/2022	Fecha de actualización	10/08/2022

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa/Unidad Administrativa.	
Identificador único	SA_UA_CA
Nombre del sistema	Control de Acceso
Datos personales	Nombre Huella Digital (sensible)
Responsable	
Nombre	César Ávalos Hernández
Cargo	Jefe de Unidad Administrativa
Funciones	Dar de alta/baja al personal que se autorice su ingreso.
Obligaciones	Mantener la operación del control de acceso. Resguardar la información del sistema.
Encargados	
Nombre	NO HAY
Usuarios	
Nombre	NO HAY

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

Tipo de soporte	Electrónico
Descripción	Access Pro S/M
Características del lugar donde se resguardan los soportes	Oficina con cerradura. Computadora con contraseña.

3. ANÁLISIS DE RIESGOS

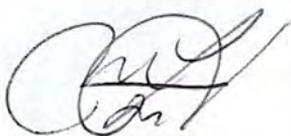
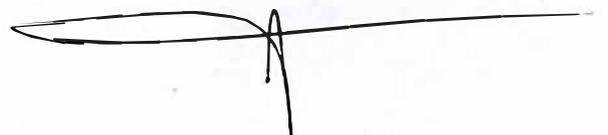
INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Transferencias mediante el traslado de soportes físicos:	NO HAY
Transferencias mediante el traslado de soportes electrónicos:	Existe traslado por respaldo
Transferencias mediante el traslado sobre redes electrónicas:	NO HAY

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

No existen soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No existe bitácora. Cuando se autoriza el acceso a las instalaciones o suprimir el acceso, el responsable tramita el alta o baja en el sistema.

IV. REGISTRO DE INCIDENTES

- El responsable elabora informe del incidente.
- En caso de robo o extravío, el responsable del sistema da vista al titular de la dependencia para su conocimiento y en el ámbito de sus atribuciones, determine lo conducente.
- En caso de robo o extravío, el responsable deberá alertar a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información.

V. ACCESO A LAS INSTALACIONES

I. Seguridad perimetral exterior

- Se tiene control de acceso a las oficinas.
- El personal autorizado accede mediante su huella digital.
- Se cuenta con circuito cerrado de TV en los accesos

2. Seguridad perimetral interior

- Oficina con cerradura.
- Computadora con contraseña.

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

La información se actualiza cuando se tiene que dar de alta/baja al personal que se autorice su ingreso.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El responsable es el único usuario y modifica su contraseña periódicamente.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Quando se aplica un alta/baja del personal, el responsable respalda la información en un dispositivo externo que resguarda en una oficina diferente.

IX. PLAN DE CONTINGENCIA

En caso de alguna contingencia se recupera el sistema a través del respaldo.
No se cuenta con sitio alterno.

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

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

Recurso	Descripción	Control
ESET Endpoint Security	Antivirus	Automático

7.2. Procedimiento para la revisión de las medidas de seguridad

Medida de seguridad	Procedimiento	Responsable
Lector de acceso	Verificar su funcionamiento	César Ávalos Hernández Diario

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

Medida de seguridad	Resultado de evaluación	Responsable
Lector de acceso	En funcionamiento	César Ávalos Hernández Diario

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

Medida de seguridad	Acciones	Responsable
Lector de acceso	Mantenimiento correctivo Mantenimiento preventivo	César Ávalos Hernández

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

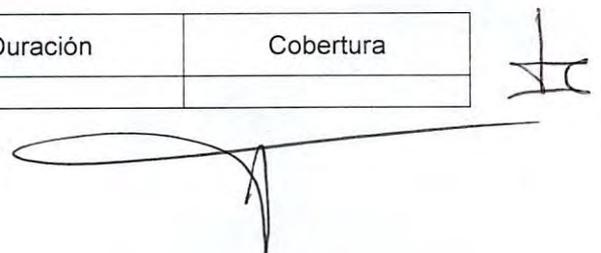
8.2. Programa de difusión de la protección a los datos personales

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Actividad	Descripción	Duración	Cobertura
NINGUNA			



9.2. Actualización y mantenimiento de equipo de cómputo

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Proceso	Descripción	Responsable
Respaldo	Cuando ocurre una alta o baja se respalda en un dispositivo externo	César Ávalos Hernández Un día

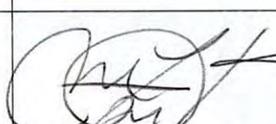
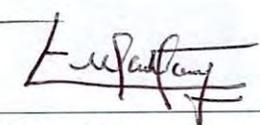
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Proceso	Descripción	Responsable
Borrado seguro	Conforme a la Circular DGTIC/003/2017	Mayra Téllez Hernández
Baja de equipo y/o componentes	Trámite de Baja emitido por la DG del Patrimonio Universitario	Nayeli Hernández Martínez

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

No existe procedimiento de cancelación, en virtud de que los datos personales recabados son exclusivamente para permitir el acceso a las instalaciones y no se tiene previsto la cancelación del sistema.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

	Desarrolló	Revisó	Autorizó
Nombre	Mayra Téllez Hernández	César Ávalos Hernández	Eduardo Maristany Cáceres
Puesto	Jefe de Departamento	Jefe de Unidad Administrativa	Responsable de seguridad de datos personales
Teléfono	55 5622 1350	55 5622 1330	55 5623 0257
Correo Electrónico	mtellezh@unam.mx	cavalosh@unam.mx	emaristany@unam.mx
Firma			
Fecha de aprobación	10/08/2022	Fecha de actualización	10/08/2022



1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa/Sede Alterna.	
Identificador único	SA_SA CCTV
Nombre del sistema	Circuito cerrado de TV
Datos personales	Imágenes (sensible)
Responsable	
Nombre	Hugo López de Lara Alatorre
Cargo	Delegado Administrativo
Funciones	Monitorear las grabaciones. En caso de incidente, notificar a las instancias correspondientes.
Obligaciones	Mantener la operación de las cámaras de video.
Encargados	
Nombre	NO HAY
Usuarios	
Nombre	NO HAY

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

Tipo de soporte	Electrónico
Descripción	Hikvision, DS-7616NI-K2/16P
Características del lugar donde se resguardan los soportes	Oficina con cerradura. Computadora con contraseña.

3. ANÁLISIS DE RIESGOS

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Transferencias mediante el traslado de soportes físicos:	NO HAY
Transferencias mediante el traslado de soportes electrónicos:	NO HAY
Transferencias mediante el traslado sobre redes electrónicas:	NO HAY

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

No existen soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No existe bitácora.

IV. REGISTRO DE INCIDENTES

- El responsable elabora informe del incidente.
- En caso de robo o extravío, el responsable del sistema da vista al titular de la dependencia para su conocimiento y en el ámbito de sus atribuciones, determine lo conducente.

V. ACCESO A LAS INSTALACIONES

I. Seguridad perimetral exterior

- Se tiene control de acceso a las oficinas.
- El personal autorizado accede mediante su huella digital.
- Se cuenta con circuito cerrado de TV en los accesos

2. Seguridad perimetral interior

- Oficina con cerradura.
- Computadora con contraseña.

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

La información se actualiza en tiempo real.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El responsable es el único usuario y modifica su contraseña periódicamente.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

No se tienen procedimientos de respaldo y recuperación de datos.

IX. PLAN DE CONTINGENCIA

No es necesario el plan de contingencia.
No se cuenta con sitio alternativo.

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

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

Recurso	Descripción	Control
ESET Endpoint Security	Antivirus	Automático

7.2. Procedimiento para la revisión de las medidas de seguridad

Medida de seguridad	Procedimiento	Responsable
Cámaras de video	Verificar su funcionamiento	Hugo López de Lara Alatorre Diario

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

Medida de seguridad	Resultado de evaluación	Responsable
Cámaras de video	En funcionamiento	Hugo López de Lara Alatorre Diario

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

Medida de seguridad	Acciones	Responsable
Cámaras de video	Mantenimiento correctivo	Hugo López de Lara Alatorre

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9.2. Actualización y mantenimiento de equipo de cómputo

Actividad	Descripción	Duración	Cobertura
-----------	-------------	----------	-----------

NINGUNA			
---------	--	--	--

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

Proceso	Descripción	Responsable
No es necesario conservar, preservar y respaldar la información		

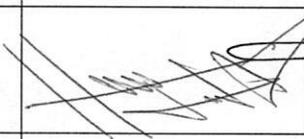
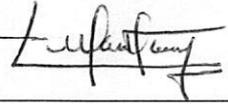
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Borrado seguro	Conforme a la Circular DGTIC/003/2017	Mayra Téllez Hernández
Baja de equipo y/o componentes	Trámite de Baja emitido por la DG del Patrimonio Universitario	Nayeli Hernández Martínez

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

No existe procedimiento de cancelación, en virtud de que los datos personales recabados son exclusivamente para seguridad de las instalaciones y no se tiene previsto la cancelación del sistema.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

	Desarrolló	Revisó	Autorizó
Nombre	Hugo López de Lara Alatorre	César Ávalos Hernández	Eduardo Maristany Cáceres
Puesto	Delegado Administrativo	Jefe de Unidad Administrativa	Responsable de seguridad de datos personales
Teléfono	55 5658 5650	55 5622 1330	55 5623 0257
Correo Electrónico	hlodela@unam.mx	cavalosh@unam.mx	emaristany@unam.mx
Firma			
Fecha de aprobación	10/08/2022	Fecha de actualización	10/08/2022

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa/Sede Alternativa.	
Identificador único	SA_SA_CA
Nombre del sistema	Control de Acceso
Datos personales	Nombre Sexo Huella Digital (sensible)
Responsable	
Nombre	Hugo López de Lara Alatorre
Cargo	Delegado Administrativo
Funciones	Dar de alta/baja al personal que se autorice su ingreso.
Obligaciones	Mantener la operación del control de acceso. Resguardar la información del sistema.
Encargados	
Nombre	NO HAY
Usuarios	
Nombre	NO HAY

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

Tipo de soporte	Electrónico
Descripción	Marca Access PRO, modelo ICLOCK-990
Características del lugar donde se resguardan los soportes	Oficina con cerradura. Computadora con contraseña.

3. ANÁLISIS DE RIESGOS

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Transferencias mediante el traslado de soportes físicos:	NO HAY
Transferencias mediante el traslado de soportes electrónicos:	Existe traslado por respaldo
Transferencias mediante el traslado sobre redes electrónicas:	NO HAY

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

No existen soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No existe bitácora. Cuando se autoriza el acceso a las instalaciones o suprimir el acceso, el responsable tramita el alta o baja en el sistema.

IV. REGISTRO DE INCIDENTES

- El responsable elabora informe del incidente.
- En caso de robo o extravío, el responsable del sistema da vista al titular de la dependencia para su conocimiento y en el ámbito de sus atribuciones, determine lo conducente.
- En caso de robo o extravío, el responsable deberá alertar a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior

- Se tiene control de acceso a las oficinas.
- El personal autorizado accede mediante su huella digital.
- Se cuenta con circuito cerrado de TV en los accesos

2. Seguridad perimetral interior

- Oficina con cerradura.
- Computadora con contraseña.

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

La información se actualiza cuando se tiene que dar de alta/baja al personal que se autorice su ingreso.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El responsable es el único usuario y modifica su contraseña periódicamente.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS



Cuando se aplica un alta/baja del personal, el responsable respalda la información en un dispositivo externo que resguarda en una oficina diferente.

IX. PLAN DE CONTINGENCIA

En caso de alguna contingencia se recupera el sistema a través del respaldo.
No se cuenta con sitio alterno.

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

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

Recurso	Descripción	Control
ESET Endpoint Security	Antivirus	Automático

7.2. Procedimiento para la revisión de las medidas de seguridad

Medida de seguridad	Procedimiento	Responsable
Lector de acceso	Verificar su funcionamiento	Hugo López de Lara Alatorre Diario

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

Medida de seguridad	Resultado de evaluación	Responsable
Lector de acceso	En funcionamiento	Hugo López de Lara Alatorre Diario

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

Medida de seguridad	Acciones	Responsable
Lector de acceso	Mantenimiento correctivo Mantenimiento preventivo	Hugo López de Lara Alatorre

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9.2. Actualización y mantenimiento de equipo de cómputo

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Proceso	Descripción	Responsable
Respaldo	Cuando ocurre una alta o baja se respalda en un dispositivo externo	Hugo López de Lara Alatorre Un día

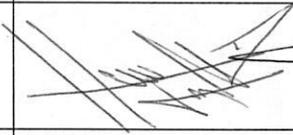
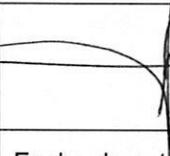
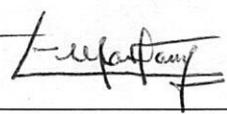
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Proceso	Descripción	Responsable
Borrado seguro	Conforme a la Circular DGTIC/003/2017	Mayra Téllez Hernández
Baja de equipo y/o componentes	Trámite de Baja emitido por la DG del Patrimonio Universitario	Nayeli Hernández Martínez

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

No existe procedimiento de cancelación, en virtud de que los datos personales recabados son exclusivamente para permitir el acceso a las instalaciones y no se tiene previsto la cancelación del sistema.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

	Desarrolló	Revisó	Autorizó
Nombre	Hugo López de Lara Alatorre	César Ávalos Hernández	Eduardo Maristany Cáceres
Puesto	Delegado Administrativo	Jefe de Unidad Administrativa	Responsable de seguridad de datos personales
Teléfono	55 5658 5650	55 5622 1330	55 5623 0257
Correo Electrónico	hlodela@unam.mx	cavalosh@unam.mx	emaristany@unam.mx
Firma			
Fecha de aprobación	10/08/2022	Fecha de actualización	10/08/2022

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa/ Centro de Exposiciones y Congresos.	
Identificador único	SA_CEC_CCTV
Nombre del sistema	Circuito cerrado de TV
Datos personales	Imágenes (sensible)
Responsable	
Nombre	Jorge Arturo Reyes Torres
Cargo	Delegado Administrativo
Funciones	Monitorear las grabaciones. En caso de incidente, notificar a las instancias correspondientes.
Obligaciones	Mantener la operación de las cámaras de video.
Encargados	
Nombre	NO HAY
Usuarios	
Nombre	Rafael Escartín Bojorges
Cargo	Jefe de Departamento
Funciones	Monitorear las grabaciones. En caso de incidente, notificar al responsable
Obligaciones	Mantener la operación de las cámaras de video.

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

Tipo de soporte	Electrónico
Descripción	Hikvision, DS-7732NI-K4/16P
Características del lugar donde se resguardan los soportes	Oficina con puerta reforzada y doble cerradura. Computadora con contraseña.

3. ANÁLISIS DE RIESGOS

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.





5. PLAN DE TRABAJO

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Transferencias mediante el traslado de soportes físicos:	NO HAY
Transferencias mediante el traslado de soportes electrónicos:	NO HAY
Transferencias mediante el traslado sobre redes electrónicas:	NO HAY

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

No existen soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No existe bitácora.

IV. REGISTRO DE INCIDENTES

- El responsable elabora informe del incidente.
- En caso de robo o extravío, el responsable del sistema da vista al titular de la dependencia para su conocimiento y en el ámbito de sus atribuciones, determine lo conducente.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior

- Se tiene control de acceso a las oficinas.
- El personal autorizado accede mediante su clave.
- Se cuenta con circuito cerrado de TV en los accesos.

2. Seguridad perimetral interior

- Oficina con cerradura.
- Computadora con contraseña.

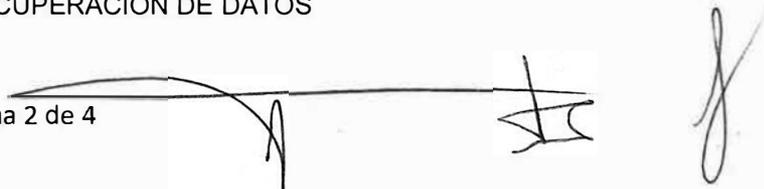
3. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La información se actualiza en tiempo real.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El responsable y el usuario modifican su contraseña periódicamente.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS



No se tienen procedimientos de respaldo y recuperación de datos.

IX. PLAN DE CONTINGENCIA

No es necesario el plan de contingencia.
No se cuenta con sitio alterno.

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

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

Recurso	Descripción	Control
ESET Endpoint Security	Antivirus	Automático

7.2. Procedimiento para la revisión de las medidas de seguridad

Medida de seguridad	Procedimiento	Responsable
Cámaras de video	Verificar su funcionamiento	Jorge Arturo Reyes Torres Diario

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

Medida de seguridad	Resultado de evaluación	Responsable
Cámaras de video	En funcionamiento	Jorge Arturo Reyes Torres Diario

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

Medida de seguridad	Acciones	Responsable
Cámaras de video	Mantenimiento correctivo	Jorge Arturo Reyes Torres

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Actividad	Descripción	Duración	Cobertura
-----------	-------------	----------	-----------

NINGUNA			
---------	--	--	--

9.2. Actualización y mantenimiento de equipo de cómputo

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Proceso	Descripción	Responsable
No es necesario conservar, preservar y respaldar la información		

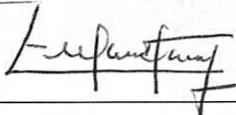
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Borrado seguro	Conforme a la Circular DGTIC/003/2017	Mayra Téllez Hernández
Baja de equipo y/o componentes	Trámite de Baja emitido por la DG del Patrimonio Universitario	Nayeli Hernández Martínez

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

No existe procedimiento de cancelación, en virtud de que los datos personales recabados son exclusivamente para seguridad de las instalaciones y no se tiene previsto la cancelación del sistema.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

	Desarrolló	Revisó	Autorizó
Nombre	Jorge Arturo Reyes Torres	César Ávalos Hernández	Eduardo Maristany Cáceres
Puesto	Delegado Administrativo	Jefe de Unidad Administrativa	Responsable de seguridad de datos personales
Teléfono	55 5622 6166	55 5622 1330	55 5623 0257
Correo Electrónico	jreyest@unam.mx	cavalosh@unam.mx	emaristany@unam.mx
Firma			
Fecha de aprobación	10/08/2022	Fecha de actualización	10/08/2022

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa/ Centro de Exposiciones y Congresos.	
Identificador único	SA_CEC_CA
Nombre del sistema	Control de Acceso
Datos personales	Nombre Huella Digital (sensible)
Responsable	
Nombre	Jorge Arturo Reyes Torres
Cargo	Delegado Administrativo
Funciones	Dar de alta/baja al personal que se autorice su ingreso.
Obligaciones	Mantener la operación del control de acceso. Resguardar la información del sistema.
Encargados	
Nombre	NO HAY
Usuarios	
Nombre	NO HAY

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

Tipo de soporte	Electrónico
Descripción	ZKTeco, Modelo: X7
Características del lugar donde se resguardan los soportes	Oficina con cerradura. Computadora con contraseña.

3. ANÁLISIS DE RIESGOS

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Transferencias mediante el traslado de soportes físicos:	NO HAY
Transferencias mediante el traslado de soportes electrónicos:	Existe traslado por respaldo
Transferencias mediante el traslado sobre redes electrónicas:	NO HAY

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

No existen soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No existe bitácora. Cuando se autoriza el acceso a las instalaciones o suprimir el acceso, el responsable tramita el alta o baja en el sistema a través del proveedor que hace el mantenimiento.

IV. REGISTRO DE INCIDENTES

- El responsable elabora informe del incidente.
- En caso de robo o extravío, el responsable del sistema da vista al titular de la dependencia para su conocimiento y en el ámbito de sus atribuciones, determine lo conducente.
- En caso de robo o extravío, el responsable deberá alertar a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior

- Se tiene control de acceso a las oficinas.
- El personal autorizado accede mediante su huella digital.
- Se cuenta con circuito cerrado de TV en los accesos

2. Seguridad perimetral interior

- Oficina con cerradura.
- Computadora con contraseña.

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

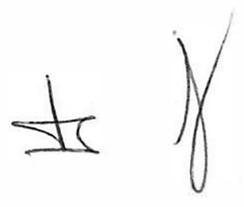
La información se actualiza cuando se tiene que dar de alta/baja al personal que se autorice su ingreso.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El responsable es el único usuario y modifica su contraseña periódicamente.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Cuando se aplica un alta/baja del personal, el responsable respalda la información en un dispositivo externo que resguarda en una oficina diferente.



IX. PLAN DE CONTINGENCIA

En caso de alguna contingencia se recupera el sistema a través del respaldo.
No se cuenta con sitio alerno.

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

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

Recurso	Descripción	Control
ESET Endpoint Security	Antivirus	Automático

7.2. Procedimiento para la revisión de las medidas de seguridad

Medida de seguridad	Procedimiento	Responsable
Lector de acceso	Verificar su funcionamiento	Jorge Arturo Reyes Torres Diario

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

Medida de seguridad	Resultado de evaluación	Responsable
Lector de acceso	En funcionamiento	Jorge Arturo Reyes Torres Diario

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

Medida de seguridad	Acciones	Responsable
Lector de acceso	Mantenimiento correctivo Mantenimiento preventivo	Jorge Arturo Reyes Torres

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9.2. Actualización y mantenimiento de equipo de cómputo

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Proceso	Descripción	Responsable
Respaldo	Cuando ocurre una alta o baja se respalda en un dispositivo externo	Jorge Arturo Reyes Torres Un día

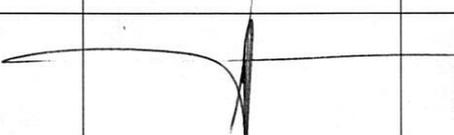
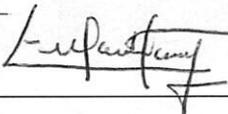
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Proceso	Descripción	Responsable
Borrado seguro	Conforme a la Circular DGTIC/003/2017	Mayra Téllez Hernández
Baja de equipo y/o componentes	Trámite de Baja emitido por la DG del Patrimonio Universitario	Nayeli Hernández Martínez

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

No existe procedimiento de cancelación, en virtud de que los datos personales recabados son exclusivamente para permitir el acceso a las instalaciones y no se tiene previsto la cancelación del sistema.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

	Desarrolló	Revisó	Autorizó
Nombre	Jorge Arturo Reyes Torres	César Ávalos Hernández	Eduardo Maristany Cáceres
Puesto	Delegado Administrativo	Jefe de Unidad Administrativa	Responsable de seguridad de datos personales
Teléfono	55 5622 6166	55 5622 1330	55 5623 0257
Correo Electrónico	jreyest@unam.mx	cavalosh@unam.mx	emaristany@unam.mx
Firma			
Fecha de aprobación	10/08/2022	Fecha de actualización	10/08/2022

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa/Unidad Administrativa/Unidad de Coordinación Administrativa.	
Identificador único	SA UA UCA CCTV
Nombre del sistema	Circuito cerrado de TV
Datos personales	Imágenes (sensible)
Responsable	
Nombre	María del Carmen Gómez Corral
Cargo	Delegado
Funciones	Monitorear las grabaciones. En caso de incidente, notificar a las instancias correspondientes.
Obligaciones	Mantener la operación de las cámaras de video.
Encargados	
Nombre	NO HAY
Usuarios	
Nombre	NO HAY

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

Tipo de soporte	Electrónico
Descripción	Hikvision, Modelo IVMS 4200 Lite
Características del lugar donde se resguardan los soportes	Oficina con cerradura. Computadora con contraseña.

3. ANÁLISIS DE RIESGOS

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Transferencias mediante el traslado de soportes físicos:	NO HAY
Transferencias mediante el traslado de soportes electrónicos:	NO HAY
Transferencias mediante el traslado sobre redes electrónicas:	NO HAY

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

No existen soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No existe bitácora.

IV. REGISTRO DE INCIDENTES

- El responsable elabora informe del incidente.
- En caso de robo o extravío, el responsable del sistema da vista al titular de la dependencia para su conocimiento y en el ámbito de sus atribuciones, determine lo conducente.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior

- Se tienen dos controles de acceso (uno al edificio y otro a las oficinas), con intercomunicador mediante el cual se identifica a la persona que quiere acceder.
- El personal autorizado accede mediante su huella digital.
- Se cuenta con circuito cerrado de TV en los accesos

2. Seguridad perimetral interior

- Oficina con cerradura.
- Computadora con contraseña.

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

La información se actualiza en tiempo real.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El responsable es el único usuario y modifica su contraseña periódicamente.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

No se tienen procedimientos de respaldo y recuperación de datos.

IX. PLAN DE CONTINGENCIA

No es necesario el plan de contingencia.

No se cuenta con sitio alterno.

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

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

Recurso	Descripción	Control
ESET Endpoint Security	Antivirus	Automático

7.2. Procedimiento para la revisión de las medidas de seguridad

Medida de seguridad	Procedimiento	Responsable
Cámaras de video	Verificar su funcionamiento	María del Carmen Gómez Corral Diario

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

Medida de seguridad	Resultado de evaluación	Responsable
Cámaras de video	En funcionamiento	María del Carmen Gómez Corral Diario

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

Medida de seguridad	Acciones	Responsable
Cámaras de video	Mantenimiento correctivo	María del Carmen Gómez Corral

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

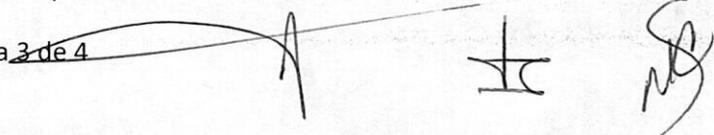
Actividad	Descripción	Duración	Cobertura
NINGUNA			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9.2. Actualización y mantenimiento de equipo de cómputo



Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Proceso	Descripción	Responsable
No es necesario conservar, preservar y respaldar la información		

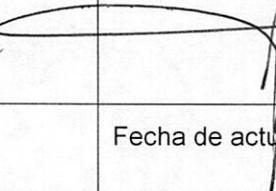
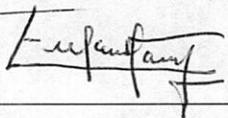
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Borrado seguro	Conforme a la Circular DGTIC/003/2017	Mayra Téllez Hernández
Baja de equipo y/o componentes	Trámite de Baja emitido por la DG del Patrimonio Universitario	Nayeli Hernández Martínez

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

No existe procedimiento de cancelación, en virtud de que los datos personales recabados son exclusivamente para seguridad de las instalaciones y no se tiene previsto la cancelación del sistema.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

	Desarrolló	Revisó	Autorizó
Nombre	María del Carmen Gómez Corral	César Ávalos Hernández	Eduardo Maristany Cáceres
Puesto	Delegada	Jefe de Unidad Administrativa	Responsable de seguridad de datos personales
Teléfono	55 5622 0833	55 5622 1330	55 5623 0257
Correo Electrónico	mgcorral@unam.mx	cavalosh@unam.mx	emaristany@unam.mx
Firma			
Fecha de aprobación	10/08/2022	Fecha de actualización	10/08/2022

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa/Unidad Administrativa/Unidad de Coordinación Administrativa.	
Identificador único	SA_UA_UCA_CA
Nombre del sistema	Control de Acceso
Datos personales	Nombre Sexo Huella Digital (sensible)
Responsable	
Nombre	María del Carmen Gómez Corral
Cargo	Delegado
Funciones	Dar de alta/baja al personal que se autorice su ingreso.
Obligaciones	Mantener la operación del control de acceso. Resguardar la información del sistema.
Encargados	
Nombre	NO HAY
Usuarios	
Nombre	NO HAY

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

Tipo de soporte	Electrónico
Descripción	Marca ZKTOCO, Modelo G3h
Características del lugar donde se resguardan los soportes	Oficina con cerradura. Computadora con contraseña.

3. ANÁLISIS DE RIESGOS

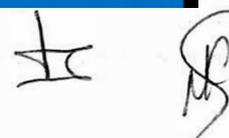
INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.



6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Transferencias mediante el traslado de soportes físicos:	NO HAY
Transferencias mediante el traslado de soportes electrónicos:	Existe traslado por respaldo
Transferencias mediante el traslado sobre redes electrónicas:	NO HAY

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

No existen soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No existe bitácora. Cuando se autoriza el acceso a las instalaciones o suprimir el acceso, el responsable tramita el alta o baja en el sistema.

IV. REGISTRO DE INCIDENTES

- El responsable elabora informe del incidente.
- En caso de robo o extravío, el responsable del sistema da vista al titular de la dependencia para su conocimiento y en el ámbito de sus atribuciones, determine lo conducente.
- En caso de robo o extravío, el responsable deberá alertar a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior

- Se tienen dos controles de acceso (uno al edificio y otro a las oficinas), con intercomunicador mediante el cual se identifica a la persona que quiere acceder.
- El personal autorizado accede mediante su huella digital.
- Se cuenta con circuito cerrado de TV en los accesos

2. Seguridad perimetral interior

- Oficina con cerradura.
- Computadora con contraseña.

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

La información se actualiza cuando se tiene que dar de alta/baja al personal que se autorice su ingreso.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El responsable es el único usuario y modifica su contraseña periódicamente.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS



Cuando se aplica un alta/baja del personal, el responsable respalda la información en un dispositivo externo que resguarda en una oficina diferente.

IX. PLAN DE CONTINGENCIA

En caso de alguna contingencia se recupera el sistema a través del respaldo.
No se cuenta con sitio alternativo.

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

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

Recurso	Descripción	Control
ESET Endpoint Security	Antivirus	Automático

7.2. Procedimiento para la revisión de las medidas de seguridad

Medida de seguridad	Procedimiento	Responsable
Lector de acceso	Verificar su funcionamiento	María del Carmen Gómez Corral Diario

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

Medida de seguridad	Resultado de evaluación	Responsable
Lector de acceso	En funcionamiento	María del Carmen Gómez Corral Diario

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

Medida de seguridad	Acciones	Responsable
Lector de acceso	Mantenimiento correctivo Mantenimiento preventivo	María del Carmen Gómez Corral

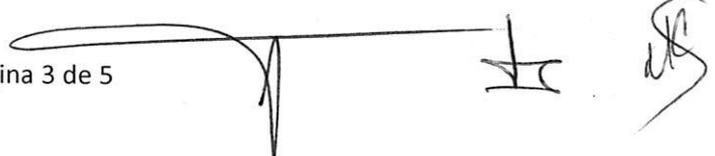
8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			



9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9.2. Actualización y mantenimiento de equipo de cómputo

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Proceso	Descripción	Responsable
Respaldo	Cuando ocurre una alta o baja se respalda en un dispositivo externo	María del Carmen Gómez Corral Un día

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

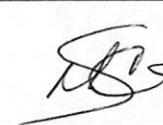
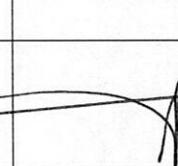
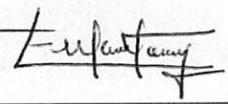
Proceso	Descripción	Responsable
Borrado seguro	Conforme a la Circular DGTIC/003/2017	Mayra Téllez Hernández
Baja de equipo y/o componentes	Trámite de Baja emitido por la DG del Patrimonio Universitario	Nayeli Hernández Martínez

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

No existe procedimiento de cancelación, en virtud de que los datos personales recabados son exclusivamente para permitir el acceso a las instalaciones y no se tiene previsto la cancelación del sistema.



11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

	Desarrolló	Revisó	Autorizó
Nombre	María del Carmen Gómez Corral	César Ávalos Hernández	Eduardo Maristany Cáceres
Puesto	Delegada	Jefe de Unidad Administrativa	Responsable de seguridad de datos personales
Teléfono	55 5622 0833	55 5622 1330	55 5623 0257
Correo Electrónico	mgcorral@unam.mx	cavalosh@unam.mx	emaristany@unam.mx
Firma			
Fecha de aprobación	10/08/2022	Fecha de actualización	10/08/2022



1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Secretaría Administrativa/Unidad de Seminarios "Ignacio Chávez".	
Identificador único	SA_US_CCTV
Nombre del sistema	Circuito cerrado de TV
Datos personales	Imágenes (sensible)
Responsable	
Nombre	Gloria Eloísa Boyce y Walker
Cargo	Coordinadora
Funciones	Monitorear las grabaciones. En caso de incidente, notificar a las instancias correspondientes.
Obligaciones	Mantener la operación de las cámaras de video.
Encargados	
Nombre	NO HAY
Usuarios	
Nombre	Miguel Ángel Pereira Sánchez
Cargo	Multicopista
Funciones	Monitorear las grabaciones. En caso de incidente, notificar al responsable
Obligaciones	Mantener la operación de las cámaras de video.

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

Tipo de soporte	Electrónico
Descripción	Hikvision, DS-7716NI-K4/16P
Características del lugar donde se resguardan los soportes	Oficina con cerradura. Computadora con contraseña.

3. ANÁLISIS DE RIESGOS

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

4. ANÁLISIS DE BRECHA

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO

INFORMACIÓN RESERVADA por cinco años a partir del 24 de agosto de 2022, con fundamento en lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Transferencias mediante el traslado de soportes físicos:	NO HAY
Transferencias mediante el traslado de soportes electrónicos:	NO HAY
Transferencias mediante el traslado sobre redes electrónicas:	NO HAY

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

No existen soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

No existe bitácora.

IV. REGISTRO DE INCIDENTES

- El responsable elabora informe del incidente.
- En caso de robo o extravío, el responsable del sistema da vista al titular de la dependencia para su conocimiento y en el ámbito de sus atribuciones, determine lo conducente.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior

- Se cuenta con circuito cerrado de TV en los accesos.

2. Seguridad perimetral interior

- Oficina con cerradura.
- Computadora con contraseña.

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

La información se actualiza en tiempo real.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El responsable y el usuario modifican su contraseña periódicamente.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

No se tienen procedimientos de respaldo y recuperación de datos.

IX. PLAN DE CONTINGENCIA

No es necesario el plan de contingencia.
No se cuenta con sitio alerno.

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

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

Recurso	Descripción	Control
ESET Endpoint Security	Antivirus	Automático

7.2. Procedimiento para la revisión de las medidas de seguridad

Medida de seguridad	Procedimiento	Responsable
Cámaras de video	Verificar su funcionamiento	Gloria Eloísa Boyce y Walker Diario

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

Medida de seguridad	Resultado de evaluación	Responsable
Cámaras de video	En funcionamiento	Gloria Eloísa Boyce y Walker Diario

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

Medida de seguridad	Acciones	Responsable
Cámaras de video	Mantenimiento correctivo	Gloria Eloísa Boyce y Walker

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Actividad	Descripción	Duración	Cobertura
NINGUNA			

9.2. Actualización y mantenimiento de equipo de cómputo

Actividad	Descripción	Duración	Cobertura
NINGUNA			

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

Proceso	Descripción	Responsable
No es necesario conservar, preservar y respaldar la información		

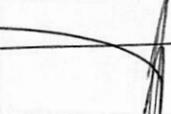
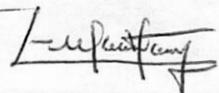
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Borrado seguro	Conforme a la Circular DGTIC/003/2017	Mayra Téllez Hernández
Baja de equipo y/o componentes	Trámite de Baja emitido por la DG del Patrimonio Universitario	Nayeli Hernández Martínez

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

No existe procedimiento de cancelación, en virtud de que los datos personales recabados son exclusivamente para seguridad de las instalaciones y no se tiene previsto la cancelación del sistema.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

	Desarrolló	Revisó	Autorizó
Nombre	Gloria Eloísa Boyce y Walker	César Ávalos Hernández	Eduardo Maristany Cáceres
Puesto	Coordinadora	Jefe de Unidad Administrativa	Responsable de seguridad de datos personales
Teléfono	55 5622 8979	55 5622 1330	55 5623 0257
Correo Electrónico	gloriabw@unam.mx	cavalosh@unam.mx	emaristany@unam.mx
Firma			
Fecha de aprobación	10/08/2022	Fecha de actualización	10/08/2022