# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

# PROGRAMA UNIVERSITARIO DE DERECHOS HUMANOS

# DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

**Octubre 2026**

# INTRODUCCIÓN

El Documento de Seguridad de Datos Personales del Programa Universitario de Derechos Humanos tiene por finalidades establecer, actualizar y reforzar las medidas de seguridad necesarias para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee esta dependencia en sus distintos sistemas de gestión, los cuales son necesarios para el cumplimiento de sus atribuciones delineadas en su Acuerdo de creación publicado en la *Gaceta UNAM* el 5 de septiembre de 2011.

El Documento de Seguridad identifica los sistemas de tratamiento de datos personales que conserva cada una de las áreas que integran el Programa. En la sección de Inventario de sistemas de tratamiento, se enuncian las funciones, obligaciones y medidas de seguridad de la personas responsables de los datos personales.

El Documento de Seguridad se mantiene actualizado, a partir del análisis de las siguientes consideraciones: la identificación de nuevas amenazas, la evaluación de posibles vulnerabilidades, la estimación de amenazas que pudieran surgir, el posible impacto de las mismas, así como el monitoreo de incidentes y vulneraciones a la seguridad. Uno de los rubros que conforma este documento es el plan de trabajo, el cual permitirá su actualización y perfeccionamiento.

El marco jurídico de la seguridad de datos personales de los que es responsable el Programa Universitario de Derechos Humanos y en el cual se fundamenta el presente documento de seguridad, se encuentra asentado en el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, cuyo apartado A, fracciones III y IV establecen los derechos toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, al acceso gratuito a la información pública, a sus datos personales o a la rectificación de los mismos; así como la obligación de que se establezcan mecanismos de acceso a la información pública y procedimientos de revisión expeditos que se sustanciarán ante las instancias competentes. En ese sentido, el presente Documento de Seguridad busca contribuir al ejercicio y de los derechos de Acceso, Rectificación, Cancelación y Oposición de datos personales, conocidos como derechos (ARCO).

Lo anterior, en relación con lo establecido en el Título segundo, Principios y Deberes, Capítulo II De los Deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el *Diario Oficial de la Federación* el 20 de marzo de 2025, donde se consagra un conjunto mínimo de medidas que cada dependencia o entidad universitaria deberá considerar al perfilar su estrategia de seguridad para la protección de los datos personales bajo su custodia, atendiendo al tipo de soportes —físicos, electrónicos o ambos— en los que residen dichos datos y se considera la protección que tales datos requieren, de conformidad con los artículos 25 a 36 de la referida Ley General.

Por lo que respecta a la Legislación Universitaria, resultan aplicables los artículos 20 al 31 de los Lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México, los cuales fueron publicados en la *Gaceta UNAM* el 25 de febrero de 2019 y los artículos 3 a 11 de las Normas Complementarias Sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, publicadas en el señalado medio de difusión el 30 de enero de 2020.

Finalmente, debe tomarse en consideración que, como parte de las estrategias permanentes para la protección de los datos, especialmente en el aspecto preventivo, la página del PUDH-UNAM: *www.pudh.com.mx* contiene documentos completos relativos a sus Avisos de Privacidad general y simplificado: *http://www.pudh.unam.mx/acuerdo_privacidad.html,*
*http://www.pudh.unam.mx/aviso_privacidad_simplificado.htm* Los mencionados avisos de privacidad hacen patentes las obligaciones de quienes en alguna u otra manera tienen contacto con los datos personales; asimismo, estos avisos reiteran las obligaciones que toda persona usuaria o servidora pública tiene respecto el manejo de la información.

## ÍNDICE

*1. Inventario de datos personales y de los sistemas de tratamiento. ..... 6*

*2. Funciones y obligaciones de las personas que tratan datos personales ..... 9*

*3. Análisis de riesgos ..... 23*

*4. Análisis de brecha ..... 31*

*5. Plan de trabajo ..... 40*

*6. Mecanismos de monitoreo y revisión de las medidas de seguridad ... 46*

**6.1 Mecanismos, herramientas y recursos para el monitoreo de la protección de datos personales ..... 46**

**6.2. Transferencias de datos personales ..... 48**

**6.3 Resguardo de sistemas de tratamiento de datos personales con soportes físicos ..... 49**

**6.4 Bitácoras para accesos y operación cotidiana ..... 49**

**6.5 Registro de incidentes ..... 50**

**6.6 Acceso a las instalaciones ..... 50**

**6.7 Actualización de la información contenida en el sistema de tratamiento de datos personales ..... 51**

**6.8 Perfiles de usuario y contraseñas ..... 51**

**6.9 Procedimientos de respaldo y recuperación de datos ..... 52**

**6.10 Plan de contingencia ..... 52**

**6.11 Procedimiento para la revisión de las medidas de seguridad ..... 53**

**6.12 Resultados de la evaluación y pruebas a las medidas de seguridad ..... 56**

**6.13 Acciones para la corrección y actualización de las medidas de seguridad .. 59**

*7. Programa general de capacitación ..... 63*

**7.1 Programa de capacitación a los responsables de la seguridad de datos personales ..... 63**

**7.2 Programa de difusión de la protección a los datos personales ..... 68**

*8 Mejora continua ..... 71*

**8.1 Actualización y mantenimiento de sistemas de información ..... 71**

**8.2 Actualización y mantenimiento de equipo de cómputo..... 75**

**8.3 Procesos para la conservación, preservación y respaldos de información.... 78**

**8.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos ..... 80**

***9. Procedimiento para la cancelación de datos personales .....84***

**Aprobación del Documento de Seguridad .....86**

## Inventario de datos personales y de los sistemas de tratamiento.

| **Departamento del Área de Sistemas** | |
|---|---|
| **Identificador único** | PUDH-WEB |
| **(Nombre del sistema A1)** | *www.pudh.unam.mx* |
| **Tipo de soporte:** | Electrónico. |
| **Descripción:** | Base de datos. |
| **Características del lugar donde se resguardan los soportes:** | Alojamiento en el Centro de Datos de la UNAM y unidad de almacenamiento externa. |

| **Archivo General del PUDH** | |
|---|---|
| **Identificador único** | PUDH-AGP |
| **(Nombre del sistema A2)** | Archivo general del PUDH |
| **Tipo de soporte:** | Físico y electrónico. |
| **Descripción:** | Hojas de cálculo.<br>Expedientes físicos. |
| **Características del lugar donde se resguardan los soportes:** | Soporte físico: Se encuentran organizados en folders debidamente clasificados almacenados en archiveros y libreros con cerradura que permiten la conservación adecuada de los documentos y se localizan resguardados por cada responsable de área del Programa.<br>Soporte electrónico: Se mantiene bajo resguardo del área de sistemas, asignando a cada persona autorizada. |

| **Delegación Administrativa** | |
|---|---|
| **Identificador único** | PUDH-SIP |
| **(Nombre del sistema A3)** | Sistema Institucional de Compras (SIP) |
| **Tipo de soporte:** | Físico y electrónico. |
| **Descripción:** | Sistema Institucional y expedientes físicos. |
| **Características del lugar donde se resguardan los soportes:** | Alojamiento en el Centro de Datos de la UNAM<br>Soporte físico: Se encuentran organizados en folders debidamente clasificados almacenados en archiveros y libreros con cerradura que permiten la conservación adecuada de los documentos. |

| | |
|---|---|
| **Delegación Administrativa** | |
| **Identificador único** | PUDH-SAI |
| **(Nombre del sistema A4)** | Sistema Institucional de Compras (SIP) |
| **Tipo de soporte:** | Físico y electrónico. |
| **Descripción:** | Sistema institucional y expedientes físicos. |
| **Características del lugar donde se resguardan los soportes:** | Alojamiento en el Centro de Datos de la UNAM Soporte físico: Se encuentran organizados en folders debidamente clasificados almacenados en archiveros y libreros con cerradura que permiten la conservación adecuada de los documentos. |

| **Delegación Administrativa** | |
|---|---|
| **Identificador único** | PUDH-SIAU WEB |
| **(Nombre del sistema A5)** | Sistema Institucional de Compras (SIP) |
| **Tipo de soporte:** | Físico y electrónico. |
| **Descripción:** | Hojas de cálculo.<br>Expedientes físicos. |
| **Características del lugar donde se resguardan los soportes:** | Alojamiento en el Centro de Datos de la UNAM Soporte físico: Se encuentran organizados en folders debidamente clasificados almacenados en archiveros y libreros con cerradura que permiten la conservación adecuada de los documentos. |

| **Departamento del Área de Sistemas** | |
|---|---|
| **Identificador único** | PUDH-WEB |
| **(Nombre del sistema A1)** | *www.pudh.unam.mx* |
| **Datos personales (sensibles o no) contenidos en el sistema:** | Datos de identificación: Nombre, celular personal, correo electrónico personal.<br><br>Datos laborales: Puesto, correo electrónico institucional, teléfono, institucional y lugar donde laboral. |

| | |
|---|---|
| | Datos académicos: Trayectoria educativa, títulos, cédulas profesionales, certificados y reconocimientos pertenecientes a cada área. |

| **Archivo General del PUDH** | |
|---|---|
| **Identificador único** | **PUDH-AGP** |
| **(Nombre del sistema A2)** | Hoja de cálculo en Excel y expedientes físicos |
| **Datos personales (sensibles o no) contenidos en el sistema:** | Datos de identificación: Nombre, celular personal, correo electrónico personal.<br><br>Datos laborales: Puesto, correo electrónico institucional, teléfono, institucional y lugar donde laboral.<br><br>Datos académicos: Trayectoria educativa, títulos, cédulas profesionales, certificados y reconocimientos pertenecientes a cada área. |

## 1. Funciones y obligaciones de las personas que tratan datos personales

| **Departamento del Área de Sistemas** | |
|---|---|
| **Identificador único** | PUDH-WEB |
| **(Nombre del sistema A1)** | *www.pudh.unam.mx* |
| **Responsable** | |
| **Nombre:** | **Lic. José Luis Belmont Lugo** |
| **Cargo:** | **Secretario Técnico** |
| **Funciones:** | Encargado de supervisar el contenido de la página web del Programa. |
| **Obligaciones:** | •Proteger los datos de los solicitantes.<br>•No modificar la información sobre datos personales provenientes de las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |
| | **Encargado:** |
| **(Nombre del Encargado 1)** | **Octavio Beltrán Estévez** |
| **Cargo:** | **Asistente de procesos** |
| **Funciones:** | •Responsable de subir información al servidor del PUDH.<br>•Encargado de sistemas computacionales y |

| | |
|---|---|
| | mantenimiento.<br>•Responsable de llevar a cabo video llamadas, grabaciones y el soporte de las comunicaciones vía remota y de los repositorios de las grabaciones. |
| **Obligaciones:** | •Proteger los datos de los solicitantes.<br>•No modificar la información de datos personales en las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados.<br>•Generar los respaldos de la información contenida en el sistema, siguiendo la política de respaldos de la Unidad de Transparencia.<br>•Mantener actualizado el servidor donde se aloja el sistema. |
| | **Usuarios:** |
| **(Nombre del Usuario 1)** | Comunidad estudiantil universitaria. |

| **Archivo General del PUDH** | |
|---|---|
| **Identificador único** | **PUDH-AGP** |
| **(Nombre del sistema A2)** | Hoja de cálculo en Excel y expedientes físicos |
| **Datos personales (sensibles o no) contenidos en el sistema:** | Datos de identificación: Nombre, celular personal, correo electrónico personal. |

| | |
|---|---|
| | Datos laborales: Puesto, correo electrónico institucional, teléfono, institucional y lugar donde laboral.<br><br>Datos académicos: Trayectoria educativa, títulos, cédulas profesionales, certificados y reconocimientos pertenecientes a cada área. |
| **Responsable:** | |
| **Nombre:** | **José Luis Belmont Lugo** |
| **Cargo:** | **Secretario Técnico** |
| **Funciones:** | Encargado de la organización y conservación, administración y preservación homogénea de los archivos generados en las áreas del Programa. |
| **Obligaciones:** | •Proteger los datos personales recabados en el sistema de tratamiento.<br>•No modificar la información de datos personales en las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |
| | **Encargados:** |
| **(Nombre del Encargado 1)** | **Rosa Nery Aguirre** |
| **Cargo:** | **Asistente de dirección** |
| **Funciones:** | •Realización de oficios, constancias y solicitudes, así como el envío de las mismas.<br>•Recibir y dar trámite a las solicitudes de información. |

| | |
|---|---|
| **Obligaciones:** | •Proteger los datos de los solicitantes.<br>•No modificar la información de datos personales en las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el sistema de tratamiento y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |
| **(Nombre del Encargado 2)** | **Adela Noemi Monroy Enriquez** |
| **Cargo:** | **Secretaria Académica** |
| **Funciones:** | •Dar seguimiento a los informes y proyectos de Investigadores que laboran en el PUDH.<br>•Resguardar y vigilar que se dé seguimiento a las solicitudes de préstamo de material de la Biblioteca.<br>•Dar acompañamiento a las personas que desean participar en el programa a través de la realización de una Estancia Posdoctoral.<br>•La realización de proyectos editoriales.<br>•La realización de instrumentos consensuales con instancias gubernamentales. |
| **Obligaciones:** | •Proteger los datos de los involucrados en todas las actividades de la Secretaría Académica.<br>•No modificar la información de datos personales en las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales |

| | |
|---|---|
| | en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |
| **(Nombre del Encargado 3)** | **Mario Naranjo Ricoy** |
| **Cargo:** | **Asistente de Secretaría Académica** |
| **Funciones:** | •Recabar la información de los proyectos de investigación del Programa.<br>•Asistir en todo el procedimiento de la biblioteca del PUDH, resguardar y dar seguimiento a las solicitudes de préstamo de material de la Biblioteca.<br>•Apoyar en la realización de Estancias Posdoctorales a los solicitantes.<br>•Auxiliar en la realización de proyectos editoriales.<br>•La realización de instrumentos consensuales con instancias gubernamentales. |
| **Obligaciones:** | •Proteger los datos de los involucrados en todas las actividades de la Secretaría Académica.<br>•No modificar la información de datos personales en las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |
| **(Nombre del Encargado 4)** | **José Luis Belmont Lugo** |
| **Cargo:** | **Secretario Técnico** |
| **Funciones:** | •Elaboración y entrega de informes (trimestrales o anuales). |

| | |
|---|---|
| | •Realizar la actualización y renovación de programas de servicio social.<br>•Entrega de solicitudes de Transparencia. |
| **Obligaciones:** | •Proteger los datos de las personas involucradas en los informes y actividades de la Secretaría Técnica.<br>•No modificar la información de datos personales en las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |
| **(Nombre del Encargado 6)** | **Yadira Alicia Gallardo Guillén** |
| **Cargo:** | **Delegada Administrativa** |
| **Funciones:** | •Elaboración y alta de contratos (en soporte físico y virtual).<br>•Elaboración y entrega de informes e indicadores (trimestrales o anuales).<br>•Supervisión y manejo de sistemas y resguardo de información a través del sistema SAI, SIP y SIAUWEB. |
| **Obligaciones:** | •Proteger los datos de los involucrados en las actividades de la Delegación Administrativa.<br>•No modificar la información de datos personales en las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con |

| | |
|---|---|
| | los lineamientos y permisos que han sido otorgados. |
| **(Nombre del Encargado 7)** | **Consuelo del Rocío Gallardo Guillén** |
| **Cargo:** | **Asistente de la Delegación Administrativa** |
| **Funciones:** | •Asistir en todos los procesos de elaboración: pago de prestadores de servicios profesionales, personal y proveedores, elaboración y alta de contratos y manejo de sistemas y resguardo de información a través del sistema SIA, SIP y SIAUWEB. |
| **Obligaciones:** | •Proteger los datos de los solicitantes.<br>•No modificar la información de datos personales en las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |
| **(Nombre del Encargado 8)** | **Abigail Leyva Martínez** |
| **Cargo:** | **Jefa de Clínica Jurídica** |
| **Funciones:** | •Gestionar y dar seguimiento a las asesorías y litigios de los casos de representación que se acompañan en la Clínica Jurídica.<br>•Generar y sistematizar investigación documental y técnicas de entrevista a las personas usuarias.<br>•Expedir los oficios y constancias del estudiantado que participa en la Clínica en las diferentes modalidades de estancia. (Servicio social, prácticas profesionales y voluntariado). |
| **Obligaciones:** | •Proteger los datos de las personas usuarias que solicitan un servicio en la Clínica Jurídica.<br>Proteger los datos del estudiantado que |

| | |
|---|---|
| | participa en la Clínica Jurídica.<br>•No modificar la información de datos personales en las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |
| **(Nombre del Encargado 9)** | **Iván Tapia Mejía** |
| **Cargo:** | **Diseño y Difusión** |
| **Funciones:** | •Manejo de redes sociales del PUDH.<br>•Interacción con seguidores de redes sociales.<br>•Creación de contenido para redes.<br>•Difusión de eventos y actividades del PUDH.<br>•Recibir y dar trámite a las solicitudes de información. |
| **Obligaciones:** | •Proteger los datos de los usuarios de nuestras redes sociales.<br>•No modificar la información de datos personales en las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados.<br>•Salvaguardar los permisos de grabación. |

| **Delegación Administrativa** | |
|---|---|
| **Identificador único** | SISTEMA INTEGRAL DE PERSONAL(SIP) |
| **(Nombre del sistema A3)** | SISTEMA INTEGRAL DE PERSONAL(SIP) |
| **Responsable** | |
| **Nombre:** | **Lic. Yadira Alicia Gallardo Guillén** |
| **Cargo:** | **Delegada Administrativa** |
| **Funciones:** | Capturar, imprimir solicitudes, constancias, formatos, notificaciones, contratos y adendas.<br><br>Aprobar y firmar electrónicamente los movimientos de personal: alta, baja, promociones, definitividad, cambios de domicilio entre otros. |
| **Obligaciones:** | •Proteger los datos de los solicitantes.<br>•No modificar la información sobre datos personales provenientes de las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |
| | **Encargado:** |
| **(Nombre del Encargado 1)** | **Consuelo del Rocío Gallardo Guillén** |
| **Cargo:** | **Asistente de procesos** |

| | |
|---|---|
| **Funciones:** | Capturar, imprimir solicitudes, constancias, formatos, notificaciones, contratos y adendas. |
| **Obligaciones:** | •Proteger los datos de los solicitantes.<br>•No modificar la información sobre datos personales provenientes de las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |

| **Delegación Administrativa** | |
|---|---|
| **Identificador único** | SISTEMA DE ADMINISTRACIÓN INSTITUCIONAL (SAI) |
| **(Nombre del sistema A4)** | SISTEMA DE ADMINISTRACIÓN INSTITUCIONAL (SAI) |
| **Responsable** | |
| **Nombre:** | **Lic. Yadira Alicia Gallardo Guillén** |
| **Cargo:** | **Delegada Administrativa** |
| **Funciones:** | • Vigilar la adquisición de bienes e insumos requeridos para las diferentes áreas a través de la Dirección General de Proveeduría o en su caso, a través de compra directa con el proveedor de acuerdo a la normatividad en materia de adquisiciones, arrendamiento y servicios |

| | |
|---|---|
| | de la UNAM Y en materia administrativa para dependencias universitarias.<br>• Revisar las solicitudes internas de compra generadas.<br>• Generar solicitudes de compra.<br>• Aprobar y firmar electrónicamente las solicitados de compra. |
| **Obligaciones:** | •Proteger los datos de los solicitantes.<br>•No modificar la información sobre datos personales provenientes de las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |
| | **Encargado:** |
| **(Nombre del Encargado 1)** | **Consuelo del Rocío Gallardo Guillén** |
| **Cargo:** | **Asistente de procesos** |
| **Funciones:** | • Vigilar la adquisición de bienes e insumos requeridos para las diferentes áreas a través de la Dirección General de Proveeduría o en su caso, a través de compra directa con el proveedor de acuerdo a la normatividad en materia de adquisiciones, arrendamiento y servicios de la UNAM Y en materia administrativa para dependencias universitarias.<br>• Revisar las solicitudes internas de compra generadas. |

| | |
|---|---|
| | • Generar solicitudes de compra. |
| **Obligaciones:** | •Proteger los datos de los solicitantes.<br>•No modificar la información sobre datos personales provenientes de las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |

| **Delegación Administrativa** | |
|---|---|
| **Identificador único** | Sistema de Información de la Administración Universitaria(SIAUWEB) |
| **(Nombre del sistema A5)** | Sistema de Información de la Administración Universitaria(SIAUWEB) |
| **Responsable** | |
| **Nombre:** | **Lic. Yadira Alicia Gallardo Guillén** |
| **Cargo:** | **Delegada Administrativa** |
| **Funciones:** | Capturar, imprimir solicitudes, constancias, formatos, notificaciones, contratos y adendas.<br><br>Aprobar y firmar electrónicamente los movimientos de personal: alta, baja, |

| | |
|---|---|
| | promociones, definitividad, cambios de domicilio entre otros. |
| **Obligaciones:** | •Proteger los datos de los solicitantes.<br>•No modificar la información sobre datos personales provenientes de las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |
| | |
| **(Nombre del Encargado 1)** | |
| **Cargo:** | No aplica, ya que no se cuenta con instrumentos consensuales suscritos con terceros para el tratamiento de los datos personales contenidos en el Sistema. |
| **Funciones:** | |
| **Obligaciones:** | |
| **Usuarios** | |
| **Nombre del Usuario 1** | **Yadira Alicia Gallardo Guillén** |
| **Cargo:** | **Delegada Administrativa** |
| **Funciones:** | **Consulta en línea de la información presupuestal y de gestión.** |
| **Obligaciones:** | •Proteger los datos de los solicitantes.<br>•No modificar la información sobre datos personales provenientes de las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a |

| | |
|---|---|
| | personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |
| **Usuarios** | |
| **Nombre del Usuario 1** | **Consuelo del Rocío Gallardo Guillén** |
| **Cargo:** | **Delegada Administrativa** |
| **Funciones:** | **Consulta en línea de la información presupuestal y de gestión.** |
| **Obligaciones:** | •Proteger los datos de los solicitantes.<br>•No modificar la información sobre datos personales provenientes de las solicitudes de información.<br>•No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.<br>•Mantener la información de datos personales en el servidor de la Unidad, en los discos duros de respaldo y no generar copias de los documentos en sus equipos de trabajo.<br>•Utilizar el sistema de gestión de acuerdo con los lineamientos y permisos que han sido otorgados. |

[redacted]

| [redacted] | | |
|---|---|---|
| [redacted] | [redacted] | |
| [redacted] | [redacted] | |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |

Análisis de riesgos, de acuerdo con la resolución CTUNAM/ 511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: el Análisis de Riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas que permitirían a determinadas personas implementar un ataque informático a los activos críticos y no críticos.

| | | |
|---|---|---|
| | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |

Análisis de riesgos, de acuerdo con la resolución CTUNAM/ 511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

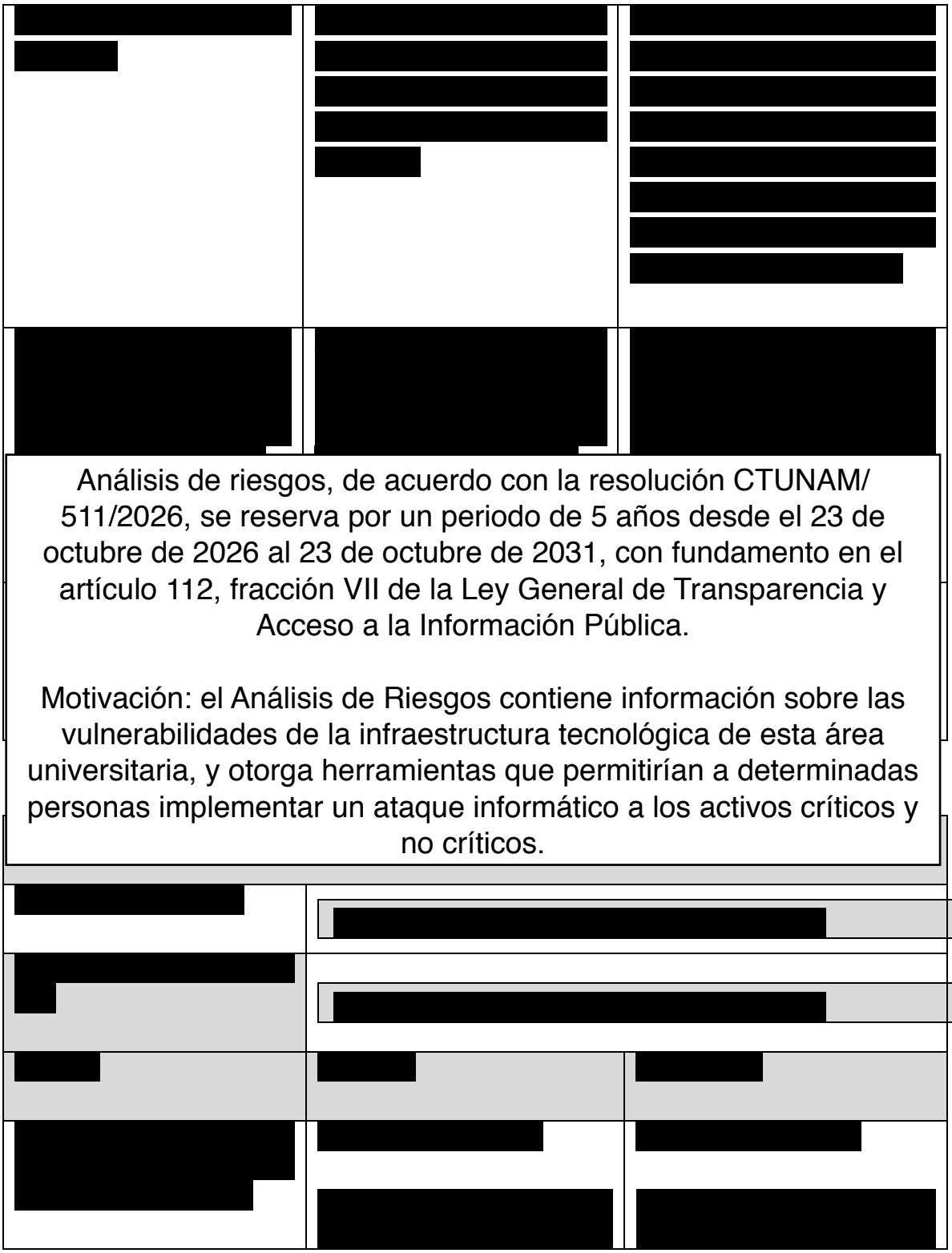
Motivación: el Análisis de Riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas que permitirían a determinadas personas implementar un ataque informático a los activos críticos y no críticos.

| | | |
|---|---|---|
| | [redacted] | [redacted] |
| | [redacted] | [redacted] |
| | [redacted] | |
| | Análisis de riesgos, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.<br><br>Motivación: el Análisis de Riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas que permitirían a determinadas personas implementar un ataque informático a los activos críticos y no críticos. | |
| [redacted] | | [redacted] |
| [redacted] | [redacted] | [redacted] |

[redacted]

Análisis de riesgos, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: el Análisis de Riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas que permitirían a determinadas personas implementar un ataque informático a los activos críticos y no críticos.



Análisis de riesgos, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: el Análisis de Riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas que permitirían a determinadas personas implementar un ataque informático a los activos críticos y no críticos.

| | | |
|---|---|---|
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |

Análisis de riesgos, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: el Análisis de Riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas que permitirían a determinadas personas implementar un ataque informático a los activos críticos y no críticos.

| | | |
|---|---|---|
| | | |
| | | |

| | | |
|---|---|---|
| [redacted] | | |
| | Análisis de riesgos, de acuerdo con la resolución CTUNAM/ 511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.<br><br>Motivación: el Análisis de Riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas que permitirían a determinadas personas implementar un ataque informático a los activos críticos y no críticos. | |
| | | |
| | | |

| | | |
|---|---|---|
| [redacted] | | |

Análisis de riesgos, de acuerdo con la resolución CTUNAM/ 511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: el Análisis de Riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas que permitirían a determinadas personas implementar un ataque informático a los activos críticos y no críticos.

[redacted]

| [redacted] | | |
|---|---|---|
| [redacted] | [redacted] | |
| [redacted] | [redacted] | |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |

Análisis de brecha, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: integra información relativa a la seguridad de la infraestructura tecnológica, controles de seguridad del área y señala las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.

| | | |
|---|---|---|
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| Análisis de brecha, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.<br><br>Motivación: integra información relativa a la seguridad de la infraestructura tecnológica, controles de seguridad del área y señala las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información. | | |
| | | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |

| | | |
|---|---|---|
| [redacted] | | [redacted] |
| Análisis de brecha, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.<br><br>Motivación: integra información relativa a la seguridad de la infraestructura tecnológica, controles de seguridad del área y señala las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información. | | |
| [redacted] | [redacted] | [redacted] |

| [redacted] | |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |

| | | |
|---|---|---|
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |

Análisis de brecha, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: integra información relativa a la seguridad de la infraestructura tecnológica, controles de seguridad del área y señala las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.

| | | |
|---|---|---|
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |

Análisis de brecha, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: integra información relativa a la seguridad de la infraestructura tecnológica, controles de seguridad del área y señala las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.

| | | |
|---|---|---|
| [redacted] | [redacted] | [redacted] |
| Análisis de brecha, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.<br><br>Motivación: integra información relativa a la seguridad de la infraestructura tecnológica, controles de seguridad del área y señala las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información. | | |
| [redacted] | [redacted] | [redacted] |

| | | |
|---|---|---|
| [redacted] | | |
| [redacted] | [redacted] | |
| Análisis de brecha, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.<br><br>Motivación: integra información relativa a la seguridad de la infraestructura tecnológica, controles de seguridad del área y señala las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información. | | |
| [redacted] | [redacted] | [redacted] |

| | | |
|---|---|---|
| [redacted] | [redacted] | [redacted] |
| | | |
| Análisis de brecha, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.<br><br>Motivación: integra información relativa a la seguridad de la infraestructura tecnológica, controles de seguridad del área y señala las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información. | | |
| [redacted] | [redacted] | [redacted] |

| [redacted] | |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |

| | | |
|---|---|---|
| [redacted] | [redacted] | [redacted] |
| | | |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |

Análisis de brecha, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: integra información relativa a la seguridad de la infraestructura tecnológica, controles de seguridad del área y señala las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.

| [redacted] | |
|---|---|
| [redacted] | [redacted] |

| | | |
|---|---|---|
| [redacted] | [redacted] | |
| [redacted] | [redacted] | [redacted] |
| | | |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |

Análisis de brecha, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: integra información relativa a la seguridad de la infraestructura tecnológica, controles de seguridad del área y señala las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.

**0**

[redacted]

| [redacted] | | | |
|---|---|---|---|
| [redacted] | [redacted] | | |
| [redacted] | [redacted] | | |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| | Plan de trabajo, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.<br><br>Motivación: el pan de trabajo define los controles a implementar de acuerdo con el resultado de los análisis de riesgo y de brecha y prioriza las medidas de seguridad de acuerdo con los riesgos reales. | | |
| | [redacted] | | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| | [redacted] | | |

| | | | |
|---|---|---|---|
| | [redacted] | | |
| [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |
| | [redacted] | | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |

Plan de trabajo, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: el pan de trabajo define los controles a implementar de acuerdo con el resultado de los análisis de riesgo y de brecha y prioriza las medidas de seguridad de acuerdo con los riesgos reales.

[redacted]

Plan de trabajo, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: el pan de trabajo define los controles a implementar de acuerdo con el resultado de los análisis de riesgo y de brecha y prioriza las medidas de seguridad de acuerdo con los riesgos reales.

[redacted]

| | | | |
|---|---|---|---|
| | [redacted] | | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] |

| | | | |
|---|---|---|---|
| Plan de trabajo, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.<br><br>Motivación: el pan de trabajo define los controles a implementar de acuerdo con el resultado de los análisis de riesgo y de brecha y prioriza las medidas de seguridad de acuerdo con los riesgos reales. | | | |
| [redacted] | | | |
| [redacted] | [redacted] | | |
| [redacted] | [redacted] | | |

| | | | |
|---|---|---|---|
| [redacted] | | | |

| | |
|---|---|
| [redacted] | |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

Plan de trabajo, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: el pan de trabajo define los controles a implementar de acuerdo con el resultado de los análisis de riesgo y de brecha y prioriza las medidas de seguridad de acuerdo con los riesgos reales.

| | | | |
|---|---|---|---|
| [redacted] | [redacted] | | |

| | |
|---|---|
| [redacted] | |
| [redacted] | [redacted] |

| | |
|---|---|
| [redacted] | [redacted] |
| Plan de trabajo, de acuerdo con la resolución CTUNAM/511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.<br><br>Motivación: el pan de trabajo define los controles a implementar de acuerdo con el resultado de los análisis de riesgo y de brecha y prioriza las medidas de seguridad de acuerdo con los riesgos reales. | |
| [redacted] | [redacted] |

## 5. Mecanismos de monitoreo y revisión de las medidas de seguridad

### 6.1 Mecanismos, herramientas y recursos para el monitoreo de la protección de datos personales

| **Departamento del área de Sistemas** | | |
|---|---|---|
| **Identificador único** | PUDH-WEB | |
| **(Nombre del sistema A1)** | *www.pudh.unam.mx* | |
| **Recurso** | **Descripción** | **Control** |
| Asignación de roles y permisos. | Administrar tipo y nivel de acceso a cada usuario. | Definición por jerarquía y consultas de información. |
| Cliente MySQL. | Se utiliza para supervisar (cuando sea solicitado) cada inicio de sesión al sistema. | Mediante credenciales de usuario y contraseña válida y activa. |

| **Archivo General del PUDH** | | |
|---|---|---|
| **Identificador único** | PUDH-AGP | |
| **(Nombre del sistema A2)** | Archivo General del PUDH | |
| **Recurso** | **Descripción** | **Control** |

| | | |
|---|---|---|
| El lector de bitácoras. | Consultas supervisadas bajo demanda. | Uso de credenciales de acceso con permisos de administrador. |

| **Delegación Administrativa** | | |
|---|---|---|
| **Identificador único** | SISTEMA INTEGRAL DE PERSONAL (SIP) | |
| **(Nombre del sistema A3)** | SISTEMA INTEGRAL DE PERSONAL (SIP) | |
| **Recurso** | **Descripción** | **Control** |
| Asignación de roles y permisos. | Administrar tipo y nivel de acceso a cada usuario. | Definición por jerarquía y consultas de información. |

| **Delegación Administrativa** | | |
|---|---|---|
| **Identificador único** | SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI) | |
| **(Nombre del sistema A4)** | SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI) | |
| **Recurso** | **Descripción** | **Control** |
| Asignación de roles y permisos. | Administrar tipo y nivel de acceso a cada usuario. | Definición por jerarquía y consultas de información. |

| | | |
|---|---|---|
| Cliente MySQL. | Se utiliza para supervisar (cuando sea solicitado) cada inicio de sesión al sistema. | Mediante credenciales de usuario y contraseña válida y activa. |

| **Delegación Administrativa** | | |
|---|---|---|
| **Identificador único** | Sistema de Información de la Administración Universitaria(SIAUWEB) | |
| **(Nombre del sistema A5)** | Sistema de Información de la Administración Universitaria(SIAUWEB) | |
| **Recurso** | **Descripción** | **Control** |
| Asignación de roles y permisos. | Administrar tipo y nivel de acceso a cada usuario. | Definición por jerarquía y consultas de información. |
| Cliente MySQL. | Se utiliza para supervisar (cuando sea solicitado) cada inicio de sesión al sistema. | Mediante credenciales de usuario y contraseña válida y activa. |

### 6.2. Transferencias de datos personales

| **Programa Universitario de Derechos Humanos** | |
|---|---|
| **Identificador único** | PUDH-WEB |
| **(Nombre del sistema A1)** | *www.pudh.unam.mx* |

| | |
|---|---|
| **Identificador único** | PUDH-AGP |
| **(Nombre del sistema A2)** | Archivo General del PUDH |

| **TRANSFERENCIAS DE DATOS PERSONALES** | |
|---|---|
| **Transferencias mediante el traslado de soportes físicos:** | Sólo se manejan entre las áreas internas del Programa. |
| **Transferencias mediante el traslado de soportes electrónicos:** | Sólo se manejan entre las áreas internas del Programa. |
| **Transferencias mediante el traslado sobre redes electrónicas:** | Sólo se realizan transferencias de datos personales a través de servicios electrónicos como el correo electrónico institucional donde se aplican las medidas de seguridad respectivas y se incluye el correspondiente aviso de privacidad. |

### 6.3 Resguardo de sistemas de tratamiento de datos personales con soportes físicos

Los soportes físicos se encuentran en fólders debidamente clasificados, en archiveros y libreros con cerradura que permiten la conservación adecuada de los documentos y el acceso está a cargo de cada responsable de área del Programa.

### 6.4 Bitácoras para accesos y operación cotidiana

**1.** El responsable de cada área debe registrar el control de usuarios para cada transacción en la base de datos, se registra fecha y hora de cada uno de los accesos a los sistemas de información.

**2.** La bitácora se resguarda en soportes electrónicos y son almacenados en el área de sistemas del Programa por lo menos 2 años en medios digitales, se crea una

copia en la nube.

**3.** Para preservar la integrar de la bitácora, se mantiene almacenada una copia de seguridad completa en soporte electrónico, la cual se encuentra bajo demanda a solicitud del Secretario Técnico.

### 6.5 Registro de incidentes

Los incidentes se reportan a cada responsable de área, elaborando un informe precisando lo acontecido. Se redacta un acta administrativa donde se describe el modo, tiempo y lugar del suceso y según las características y contenido de la información afectada. También se almacenan los archivos técnicos como referencia y soporte, el responsable del sistema debe informar al titular de la Secretaría Técnica, quienes en conocimiento ejecutarán las acciones necesarias para implementar medidas al respecto.

Todos los reportes se resguardan en carpetas locales para el registro de incidentes.

[redacted]

Acceso a las instalaciones, de acuerdo con la resolución CTUNAM/ 511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: contiene información que, de divulgarse, podría comprometer la seguridad de las instalaciones y de los datos que se resguardan al permitir inferir riesgos y vulneraciones.

[redacted]

Acceso a las instalaciones, de acuerdo con la resolución CTUNAM/ 511/2026, se reserva por un periodo de 5 años desde el 23 de octubre de 2026 al 23 de octubre de 2031, con fundamento en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Motivación: contiene información que, de divulgarse, podría comprometer la seguridad de las instalaciones y de los datos que se resguardan al permitir inferir riesgos y vulneraciones.

### 6.7 Actualización de la información contenida en el sistema de tratamiento de datos personales

La información puede ser actualizada de manera periódica de acuerdo con el calendario mensual o semestral y en base al plan de trabajo de cada área.

En el caso de que la información deba ser actualizada a petición de alguna instancia en la UNAM, se debe solicitar al titular de la Secretaría Técnica, quien remitirá al encargado del sistema, efectúe los cambios necesarios.

### 6.8 Perfiles de usuario y contraseñas

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

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

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

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

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

**a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Si
**b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si se cifran las contraseñas previamente generadas.

**4.** Administración de perfiles de usuario y contraseñas:

**a)** ¿Quién da de alta nuevos perfiles? El responsable del área de cómputo
**b)** ¿Quién autoriza la creación de nuevos perfiles? El Secretario Técnico
**c)** ¿Se lleva registro de la creación de nuevos perfiles? Si se mantiene almacenado en carpeta

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

**a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? No
**b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? Si
**c)** ¿Cómo se evita el acceso remoto no autorizado? En caso de ser necesario se hace uso de VPN

### 6.9 Procedimientos de respaldo y recuperación de datos

1. Señalar si realiza respaldos
   a) Completos _X_, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual ___X__,
   c) Periodicidad con que los realiza: __mensual_____
2. El tipo de medios que utiliza para almacenar las copias de seguridad: Fuera de línea: se utiliza un disco de estado sólido para el almacenamiento de los respaldos.
3. Cómo y dónde archiva esos medios: En su totalidad en medios físicos resguardados por el área de cómputo.
4. Quién es el responsable de realizar estas operaciones: Responsable del área de cómputo.

### 6.10 Plan de contingencia

Los sistemas de información se mantienen actualmente en operación; sin embargo, es fundamental para garantizar la continuidad y la seguridad de los datos en caso de incidentes o desastres desarrollar un Plan de contingencia.

A continuación, se indican estrategias clave para recuperar y ejecutar operaciones en los sistemas actuales:

1. Revisar y actualizar en los medios de almacenamiento se cuenten con las últimas versiones de copias de seguridad de cada área de trabajo.
2. Identificar los posibles riesgos y amenazas que podrían afectar el sistema de tratamiento de datos personales, como carpetas que contenga las versiones del sistema operativo, código fuente, información reservada o confidencial, software de la base de datos, actualizaciones, programas, archivo con la estructura de la base y datos, manual de procedimientos, entre otros.
3. Mantener el directorio de contactos actualizado con los responsables del servicio ante una posible falla en la Red UNAM y alojamiento en el Centro de Operaciones y Monitoreo NOC-UNAM para la recuperación de los servicios de tecnologías de información.
4. Tener disponible la documentación técnica detallada de las especificaciones de hardware y software, instalación de complementos de seguridad en funcion del sistema operativo, instalar las actualizaciones de seguridad más recientes disponibles, generar un inventario de claves de acceso para cada dispositivo o estación de trabajo que interactúe con los sistemas.
5. Establecer un plan de comunicación para informar a todo el personal del Programa, sobre estrategias de respuesta para cada escenario de riesgo y la implementación de medidas de mitigación en el proceso de recuperación de los servicios de tecnologías de información.
6. Establecer procedimientos de emergencia para garantizar la continuidad y seguridad de los datos personales, así como la validación de acceso seguro a los sistemas y aplicaciones en línea.
7. Realizar pruebas y simulacros del plan de contingencia para garantizar su efectividad y identificar áreas de mejora y.
8. Evaluar la efectividad integral del Plan de contingencia.

### 6.11 Procedimiento para la revisión de las medidas de seguridad

| **Departamento del Área de Sistemas** | |
|---|---|
| **Identificador único** | PUDH-WEB |
| **(Nombre del sistema A1)** | *www.pudh.unam.mx* |

| Medida de seguridad | Procedimiento | Responsable |
|---|---|---|
| Verificar actualizaciones de Software más recientes (cliente). | Comprobar nuevas versiones disponibles del cliente.<br><br>Ejecutar y actualizar paquetes existentes. | Responsable: Octavio Beltrán Estévez.<br>Tiempo de ejecución: un día. |
| Registro de información (Log del sistema). | Conservar una bitácora del historial de todas las actualizaciones mensuales de seguridad y no de seguridad publicadas para cada cliente. | Responsable: Octavio Beltrán Estévez<br>Tiempo de ejecución: un día. |

| **Archivo General del PUDH** | | |
|---|---|---|
| **Identificador único** | PUDH-AGP | |
| **(Nombre del sistema A2)** | Archivo General del PUDH | |
| **Medida de seguridad** | **Procedimiento** | **Responsable** |
| Revisión periódica de la información ingresada al equipo de cómputo. | Realizar una actualización de la información que contiene cada equipo de cómputo, en cada área del Programa. | -José Luis Belmont Lugo.<br>-Adela Noemi Monroy Enriquez.<br>-Abigail Leyva Martínez.<br>-Yadira Alicia Gallardo Guillén.<br>-Rosa Nery Aguirre.<br>-Consuelo del Rocío Gallardo Guillén.<br>-Iván Tapia Mejía.<br>-Octavio Beltrán Estévez. |

| | | |
|---|---|---|
| | | Tiempo de ejecución: 1 día por responsable. |

| **Delegación Administrativa** | | |
|---|---|---|
| **Identificador único** | *SISTEMA INTEGRAL DE PERSONAL (SIP)* | |
| **(Nombre del sistema A3)** | *SISTEMA INTEGRAL DE PERSONAL (SIP)* | |
| **Medida de seguridad** | **Procedimiento** | **Responsable** |
| | | |
| Revisión periódica de la información ingresada al equipo de cómputo. | Realizar una actualización de la información que contiene cada equipo de cómputo, en cada área del Programa. | .<br>-Yadira Alicia Gallardo Guillén.<br>-Consuelo del Rocío Gallardo Guillén.<br>. |

| **Delegación Administrativa** | | |
|---|---|---|
| **Identificador único** | *SISTEMA DE ADMINISTRTIVO INSTITUCIONAL (SAI)* | |
| **(Nombre del sistema A4)** | *SISTEMA DE ADMINISTRTIVO INSTITUCIONAL (SAI)* | |
| **Medida de seguridad** | **Procedimiento** | **Responsable** |
| | | |
| Revisión periódica de la información | Realizar una actualización de la información que | . |

| | | |
|---|---|---|
| ingresada al equipo de cómputo. | contiene cada equipo de cómputo, en cada área del Programa. | -Yadira Alicia Gallardo Guillén.<br>-Consuelo del Rocío Gallardo Guillén.<br>. |

| **Delegación Administrativa** | | |
|---|---|---|
| **Identificador único** | Sistema de Información de la Administración Universitaria(SIAUWEB) | |
| **(Nombre del sistema A5)** | Sistema de Información de la Administración Universitaria(SIAUWEB) | |
| **Medida de seguridad** | **Procedimiento** | **Responsable** |
| | | |
| Revisión periódica de la información ingresada al equipo de cómputo. | Realizar una actualización de la información que contiene cada equipo de cómputo, en cada área del Programa. | .<br>-Yadira Alicia Gallardo Guillén.<br>-Consuelo del Rocío Gallardo Guillén.<br>. |

### 6.12 Resultados de la evaluación y pruebas a las medidas de seguridad

| **Departamento del Área de Sistemas** | |
|---|---|
| **Identificador único** | PUDH-WEB |

| | | |
|---|---|---|
| **(Nombre del sistema A1)** | *www.pudh.unam.mx* | |
| **Medida de seguridad** | **Resultado de evaluación** | **Responsable** |
| Verificación de estaciones de trabajo que almacenan y ejecutan datos personales de forma local. | En consideración a los resultados, se ejecuta las acciones correspondientes. | Responsable del sistema: Octavio Beltrán Estévez.<br>Fecha de conclusión: un mes. |

| | | |
|---|---|---|
| **Archivo General del PUDH** | | |
| **Identificador único** | PUDH-AGP | |
| **(Nombre del sistema A2)** | Archivo General del PUDH | |
| **Medida de seguridad** | **Procedimiento** | **Responsable** |
| Revisión periódica de la información ingresada al equipo de cómputo. | Realizar una actualización de la información que contiene cada equipo de cómputo, en cada área del Programa. | -Consuelo del Rocío Gallardo Guillén.<br>-José Luis Belmont Lugo.<br>-Iván Tapia Mejía.<br>-Adela Noemi Monroy Enriquez.<br>-Abigail Leyva Martínez.<br>-Yadira Alicia Gallardo Guillén.<br>-Rosa Nery Aguirre.<br>-Octavio Beltrán Estévez. |
| Actualización de expedientes físicos de acuerdo a la normatividad de la UNAM. | La revisión de expedientes de cada área del Programa, así como la entrega de los expedientes correspondientes al Área de Archivos de la UNAM para tener un buen | |

| | | |
|---|---|---|
| | funcionamiento y control de los mismos. | Tiempo de ejecución: 15 días hábiles. |

| **Delegación Administrativa** | | |
|---|---|---|
| **Identificador único** | *SISTEMA INTEGRAL DE PERSONAL (SIP)* | |
| **(Nombre del sistema A3)** | *SISTEMA INTEGRAL DE PERSONAL (SIP)* | |
| **Medida de seguridad** | **Resultado de evaluación** | **Responsable** |
| Verificación de estaciones de trabajo que almacenan y ejecutan datos personales de forma local. | En consideración a los resultados, se ejecuta las acciones correspondientes. | Responsable del sistema: Octavio Beltrán Estévez.<br>Fecha de conclusión: un mes. |

| **Delegación Administrativa** | | |
|---|---|---|
| **Identificador único** | *SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI)* | |
| **(Nombre del sistema A4)** | *SISTEMA ADMINISTRATIVO INSTITUCIONAL* | |
| **Medida de seguridad** | **Resultado de evaluación** | **Responsable** |

| | | |
|---|---|---|
| Verificación de estaciones de trabajo que almacenan y ejecutan datos personales de forma local. | En consideración a los resultados, se ejecuta las acciones correspondientes. | Responsable del sistema: Octavio Beltrán Estévez.<br>Fecha de conclusión: un mes. |

| **Delegación Administrativa** | | |
|---|---|---|
| **Identificador único** | Sistema de Información de la Administración Universitaria (SIAUWEB) | |
| **(Nombre del sistema A5)** | Sistema de Información de la Administración Universitaria (SIAUWEB) | |
| **Medida de seguridad** | **Resultado de evaluación** | **Responsable** |
| Verificación de estaciones de trabajo que almacenan y ejecutan datos personales de forma local. | En consideración a los resultados, se ejecuta las acciones correspondientes. | Responsable del sistema: Octavio Beltrán Estévez.<br>Fecha de conclusión: un mes. |

### 6.13 Acciones para la corrección y actualización de las medidas de seguridad

| **Departamento del Área de Sistemas** | |
|---|---|
| **Identificador único** | PUDH-WEB |

| **(Nombre del sistema A1)** | *www.pudh.unam.mx* | |
|---|---|---|
| **Medida de seguridad** | **Acciones** | **Responsable** |
| De acuerdo con el análisis de pertenencia y factibilidad de las medidas aplicadas. | A continuación, se enlista la metodología actual:<br>• Evaluación de potenciales impactos.<br>• Identificación de necesidades.<br>• Viabilidad a corto plazo. | Octavio Beltrán Estévez.<br>Periodo: enero – junio. |

| **Archivo General del PUDH** | | |
|---|---|---|
| **Identificador único** | PUDH-AGP | |
| **(Nombre del sistema A2)** | Archivo General del PUDH | |
| **Medida de seguridad** | **Acciones** | **Responsable** |
| De acuerdo con el análisis de pertenencia y factibilidad de las medidas aplicadas. | A continuación, se enlista la metodología actual:<br>• Evaluación de potenciales impactos.<br>• Identificación de necesidades.<br>• Viabilidad a corto plazo. | -Consuelo del Rocío Gallardo Guillén.<br>-José Luis Belmont Lugo.<br>-Iván Tapia Mejía.<br>-Adela Noemi Monroy Enriquez.<br>-Octavio Beltrán Estévez.<br>-Rosa Nery Aguirre.<br>-Yadira Alicia Gallardo Guillén.<br>-Abigail Leyva Martínez.<br>-Periodo: julio – diciembre. |

| **Delegación Administrativa** | | |
|---|---|---|
| **Identificador único** | *SISTEMA INTEGRAL DE PERSONAL (SIP)* | |
| **(Nombre del sistema A3)** | *SISTEMA INTEGRAL DE PERSONAL (SIP)* | |
| **Medida de seguridad** | **Acciones** | **Responsable** |
| De acuerdo con el análisis de pertenencia y factibilidad de las medidas aplicadas. | A continuación, se enlista la metodología actual:<br>• Evaluación de potenciales impactos.<br>• Identificación de necesidades.<br>• Viabilidad a corto plazo. | Octavio Beltrán Estévez.<br>Periodo: enero – junio. |

| **Delegación Administrativa** | | |
|---|---|---|
| **Identificador único** | *SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI)* | |
| **(Nombre del sistema A4)** | *SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI)* | |
| **Medida de seguridad** | **Acciones** | **Responsable** |
| De acuerdo con el análisis de pertenencia y factibilidad de las medidas aplicadas. | A continuación, se enlista la metodología actual:<br>• Evaluación de potenciales impactos. | Octavio Beltrán Estévez.<br>Periodo: enero – junio. |

| | | |
|---|---|---|
| | • Identificación de necesidades.<br>• Viabilidad a corto plazo. | |

| **Delegación Administrativa** | | |
|---|---|---|
| **Identificador único** | Sistema de Información de la Administración Universitaria (SIAUWEB) | |
| **(Nombre del sistema A5)** | Sistema de Información de la Administración Universitaria (SIAUWEB) | |
| **Medida de seguridad** | **Acciones** | **Responsable** |
| De acuerdo con el análisis de pertenencia y factibilidad de las medidas aplicadas. | A continuación, se enlista la metodología actual:<br>• Evaluación de potenciales impactos.<br>• Identificación de necesidades.<br>• Viabilidad a corto plazo. | Octavio Beltrán Estévez.<br>Periodo: enero – junio. |

# 7. Programa general de capacitación

## 7.1 Programa de capacitación a los responsables de la seguridad de datos personales

| **Página WEB del PUDH** | | | |
|---|---|---|---|
| **Identificador único*** | PUDH-WEB | | |
| **(Nombre del sistema A1)*** | *www.pudh.unam.mx* | | |
| **Actividad*** | **Descripción*** | **Duración*** | **Cobertura*** |
| Curso introducción a la transparencia, Acceso a la información y protección de datos personales. | Sesión de videoconferencia impartida por la Subdirección de Capacitación y Evaluación de la Dirección General de Personal. | Se imparten en los meses de marzo, agosto y noviembre cubriendo 3 horas por sesión. | Dirigido al titular y responsables de datos personales: José Luis Belmont Lugo, Octavio Beltrán Estévez y Yadira Gallardo Guillén. |
| Curso de Protección de datos personales. | Sesiones vía ZOOM con pláticas y reuniones de trabajo y en oficina, con el fin de involucrar a todo el personal del Programa en la protección de los datos que se manejan. | Se impartirán cada 6 meses, en un horario de cuatro horas, durante los meses de enero y julio de cada año. | Dirigido al titular y responsables de datos personales: José Luis Belmont Lugo, Octavio Beltrán Estévez y Yadira Gallardo Guillén. |

| **Archivo General del PUDH** | | | |
|---|---|---|---|
| **Identificador único*** | PUDH-AGP | | |
| **(Nombre del sistema A2)*** | Archivo General del PUDH | | |
| **Actividad*** | **Descripción*** | **Duración*** | **Cobertura*** |
| Curso Gestión documental y organización de archivos de la UNAM. | Sesiones presenciales y virtuales, impartidas por la Subdirección de Capacitación y Evaluación de la Dirección General de Personal. | Se imparten durante 2 semanas en los meses de marzo, mayo y agosto, cubriendo 2 horas por sesión. | Dirigido al personal del PUDH-UNAM que requiera conocimientos de técnicas, herramientas, métodos y procedimientos. |
| Curso de Protección de datos personales. | Sesiones vía ZOOM con pláticas y reuniones de trabajo y en oficina con el fin de dar a conocer a todo el personal del Programa, la importancia de la protección de datos. | Se impartirán cada 6 meses en un horario de cuatro horas, en los meses de enero y julio de cada año. | Dirigido al titular y responsables de datos personales: José Luis Belmont Lugo, Octavio Beltrán Estévez y Yadira Gallardo Guillén. |
| Curso de adiestramiento, sesiones informativas y manejo de archivos | Cursos de capacitación que imparte el Área Coordinadora de Archivos, que | Se impartirán cada 6 meses en un horario de cuatro horas, en los meses de enero y julio de | Dirigido al titular y responsables de datos personales: José Luis Belmont Lugo, Octavio Beltrán Estévez y |

| | | | |
|---|---|---|---|
| físicos y electrónicos en todas sus etapas. | imparten cada año, así como el reforzamiento, a través de cursos en las instalaciones del Programa con el fin de dar a conocer a todo el personal del programa, la importancia del tema. | cada año y los cursos impartidos por el ACA, estarán sujetos al horario establecidos esta área. | Yadira Gallardo Guillén.<br><br>Vigencia: dos cursos al año. |

| **Delegación Administrativa** | | | |
|---|---|---|---|
| **Identificador único*** | SISTEMA INTEGRAL DE PERSONAL (SIP) | | |
| **(Nombre del sistema A3)*** | SISTEMA INTEGRAL DE PERSONAL (SIP) | | |
| **Actividad*** | **Descripción*** | **Duración*** | **Cobertura*** |
| Curso introducción a la transparencia, Acceso a la información y protección de datos personales. | Sesión de videoconferencia impartida por la Subdirección de Capacitación y Evaluación de la Dirección General de Personal. | Se imparten en los meses de marzo, agosto y noviembre cubriendo 3 horas por sesión. | Dirigido al titular y responsables de datos personales: José Luis Belmont Lugo, Octavio Beltrán Estévez y Yadira Gallardo Guillén. |
| Curso de Protección de datos personales. | Sesiones vía ZOOM con pláticas y reuniones de trabajo y en oficina, con el fin de | Se impartirán cada 6 meses, en un horario de cuatro horas, durante los | Dirigido al titular y responsables de datos personales: José Luis Belmont Lugo, Octavio Beltrán Estévez y |

| | | | |
|---|---|---|---|
| | involucrar a todo el personal del Programa en la protección de los datos que se manejan. | meses de enero y julio de cada año. | Yadira Gallardo Guillén. |

| **Delegación Administrativa** | | | |
|---|---|---|---|
| **Identificador único*** | SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI) | | |
| **(Nombre del sistema A4)*** | SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI) | | |
| **Actividad*** | **Descripción*** | **Duración*** | **Cobertura*** |
| Curso introducción a la transparencia, Acceso a la información y protección de datos personales. | Sesión de videoconferencia impartida por la Subdirección de Capacitación y Evaluación de la Dirección General de Personal. | Se imparten en los meses de marzo, agosto y noviembre cubriendo 3 horas por sesión. | Dirigido al titular y responsables de datos personales: José Luis Belmont Lugo, Octavio Beltrán Estévez y Yadira Gallardo Guillén. |
| Curso de Protección de datos personales. | Sesiones vía ZOOM con pláticas y reuniones de trabajo y en oficina, con el fin de involucrar a todo el personal del Programa en la protección de los | Se impartirán cada 6 meses, en un horario de cuatro horas, durante los meses de enero y julio de cada año. | Dirigido al titular y responsables de datos personales: José Luis Belmont Lugo, Octavio Beltrán Estévez y Yadira Gallardo Guillén. |

| | | | |
|---|---|---|---|
| | datos que se manejan. | | |

| **Delegación Administrativa** | | | |
|---|---|---|---|
| **Identificador único*** | Sistema de Información de la Administración Universitaria (SIAUWEB) | | |
| **(Nombre del sistema A5)*** | Sistema de Información de la Administración Universitaria (SIAUWEB) | | |
| **Actividad*** | **Descripción*** | **Duración*** | **Cobertura*** |
| Curso introducción a la transparencia, Acceso a la información y protección de datos personales. | Sesión de videoconferencia impartida por la Subdirección de Capacitación y Evaluación de la Dirección General de Personal. | Se imparten en los meses de marzo, agosto y noviembre cubriendo 3 horas por sesión. | Dirigido al titular y responsables de datos personales: José Luis Belmont Lugo, Octavio Beltrán Estévez y Yadira Gallardo Guillén. |
| Curso de Protección de datos personales. | Sesiones vía ZOOM con pláticas y reuniones de trabajo y en oficina, con el fin de involucrar a todo el personal del Programa en la protección de los | Se impartirán cada 6 meses, en un horario de cuatro horas, durante los meses de enero y julio de cada año. | Dirigido al titular y responsables de datos personales: José Luis Belmont Lugo, Octavio Beltrán Estévez y Yadira Gallardo Guillén. |

| | | | |
|---|---|---|---|
| | datos que se manejan. | | |

### 7.2 Programa de difusión de la protección a los datos personales

| **Página WEB del PUDH** | | | |
|---|---|---|---|
| **Identificador único** | PUDH-WEB | | |
| **(Nombre del sistema A1)** | *www.pudh.unam.mx* | | |
| **Actividad** | **Descripción** | **Duración** | **Cobertura** |
| Programa de actividades para la capacitación en Protección de Datos Personales. Planificación y gestión. | Reuniones de trabajo, donde se desarrollen el contenido de acciones y estrategias de acuerdo con las actividades realizadas y resultados de cada área. | Se realizarán de manera permanente, conforme a la demanda que se tenga de una hora por sesión ya sea individual o por grupos. | Dirigido a todo el personal del PUDH-UNAM. |

| **Archivo General del PUDH** | |
|---|---|
| **Identificador único** | PUDH-AGP |
| **(Nombre del sistema A2)** | Archivo General del PUDH |

| Actividad | Descripción | Duración | Cobertura |
|---|---|---|---|
| Programa de actividades de difusión, planificación y gestión sobre temas de seguridad de datos personales y transparencia. | Se difundirá contenido gráfico, infografías, carteles con acciones y estrategias de acuerdo con las actividades realizadas en cada área. | Cada dos meses se actualizará el contenido conforme a la normativa vigente. | Dirigido a todo el personal del PUDH-UNAM. |

| **Delegación Administrativa** | | | |
|---|---|---|---|
| **Identificador único** | SISTEMA INTEGRAL DE PERSONAL (SIP) | | |
| **(Nombre del sistema A3)** | SISTEMA INTEGRAL DE PERSONAL (SIP) | | |
| **Actividad** | **Descripción** | **Duración** | **Cobertura** |
| Programa de actividades para la capacitación en Protección de Datos Personales. Planificación y gestión. | Reuniones de trabajo, donde se desarrollen el contenido de acciones y estrategias de acuerdo con las actividades realizadas y resultados de cada área. | Se realizarán de manera permanente, conforme a la demanda que se tenga de una hora por sesión ya sea individual o por grupos. | Dirigido a todo el personal del PUDH-UNAM. |

| **Delegación Administrativa** | | | |
|---|---|---|---|
| **Identificador único** | SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI) | | |
| **(Nombre del sistema A4)** | SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI) | | |
| **Actividad** | **Descripción** | **Duración** | **Cobertura** |
| Programa de actividades para la capacitación en Protección de Datos Personales. Planificación y gestión. | Reuniones de trabajo, donde se desarrollen el contenido de acciones y estrategias de acuerdo con las actividades realizadas y resultados de cada área. | Se realizarán de manera permanente, conforme a la demanda que se tenga de una hora por sesión ya sea individual o por grupos. | Dirigido a todo el personal del PUDH-UNAM. |

| **Delegación Administrativa** | | | |
|---|---|---|---|
| **Identificador único** | Sistema de Información de la Administración Universitaria (SIAUWEB) | | |
| **(Nombre del sistema A5)** | Sistema de Información de la Administración Universitaria (SIAUWEB) | | |
| **Actividad** | **Descripción** | **Duración** | **Cobertura** |
| Programa de actividades para la capacitación en | Reuniones de trabajo, donde se desarrollen el contenido de acciones y | Se realizarán de manera permanente, conforme a la demanda que se | Dirigido a todo el personal del PUDH-UNAM. |

| | | | |
|---|---|---|---|
| Protección de Datos Personales. Planificación y gestión. | estrategias de acuerdo con las actividades realizadas y resultados de cada área. | tenga de una hora por sesión ya sea individual o por grupos. | |

# 8 Mejora continua

## 8.1 Actualización y mantenimiento de sistemas de información

| **Departamento del área de sistemas** | | | |
|---|---|---|---|
| **Identificador único** | PUDH-WEB | | |
| **(Nombre del sistema A1)** | *www.pudh.unam.mx* | | |
| **Actividad** | **Descripción** | **Duración** | **Cobertura** |
| Actualización del sistema operativo. | Se hace uso de la herramienta de actualización de software de macos. | En promedio de 2 a 4 horas. | Eliminación de problemas de seguridad y vulnerabilidades del sistema operativo. |
| Actualización del cliente FTP. | Se hace uso de la herramienta integrada en el sistema (*check update*). | Aproximadamente de 2 a 3 horas. | Solucionar errores de conexión SSH. |
| Renovación de Certificado de seguridad | Proceso de renovación con el Departamento Coordinación de Servicios de Identidad y Firma Electrónica | 5 días hábiles. | Anualmente |

| | | | |
|---|---|---|---|
| | Universitaria de la DGTIC. | | |

| **Archivo General del PUDH** | | | |
|---|---|---|---|
| **Identificador único** | PUDH-AGP | | |
| **(Nombre del sistema A2)** | Archivo General del PUDH | | |
| **Actividad** | **Descripción** | **Duración** | **Cobertura** |
| Actualización del sistema operativo. | Se ejecuta la herramienta *Windows update*. | Aproximadamente 2 horas. | Eliminación de vulnerabilidades del sistema. |

| **Delegación Administrativa** | | | |
|---|---|---|---|
| **Identificador único** | *SISTEMA INTEGRAL DE PERSONAL (SIP)* | | |
| **(Nombre del sistema A3)** | *SISTEMA INTEGRAL DE PERSONAL (SIP)* | | |
| **Actividad** | **Descripción** | **Duración** | **Cobertura** |
| Actualización del sistema operativo. | Se hace uso de la herramienta de actualización de software de macos. | En promedio de 2 a 4 horas. | Eliminación de problemas de seguridad y vulnerabilidades del sistema operativo. |

| | | | |
|---|---|---|---|
| Actualización del cliente FTP. | Se hace uso de la herramienta integrada en el sistema (*check update*). | Aproximadamente de 2 a 3 horas. | Solucionar errores de conexión SSH. |
| Renovación de Certificado de seguridad | Proceso de renovación con el Departamento Coordinación de Servicios de Identidad y Firma Electrónica Universitaria de la DGTIC. | 5 días hábiles. | Anualmente |

| **Delegación Administrativa** | | | |
|---|---|---|---|
| **Identificador único** | *SISTEMA ADMINISTRTIVO INSTITUCIONAL (SAI)* | | |
| **(Nombre del sistema A4)** | *SISTEMA ADMINISTRTIVO INSTITUCIONAL (SAI)* | | |
| **Actividad** | **Descripción** | **Duración** | **Cobertura** |
| Actualización del sistema operativo. | Se hace uso de la herramienta de actualización de software de macos. | En promedio de 2 a 4 horas. | Eliminación de problemas de seguridad y vulnerabilidades del sistema operativo. |
| Actualización del cliente FTP. | Se hace uso de la herramienta integrada en el sistema (*check update*). | Aproximadamente de 2 a 3 horas. | Solucionar errores de conexión SSH. |

| | | | |
|---|---|---|---|
| Renovación de Certificado de seguridad | Proceso de renovación con el Departamento Coordinación de Servicios de Identidad y Firma Electrónica Universitaria de la DGTIC. | 5 días hábiles. | Anualmente |

| **Delegación Administrativa** | | | |
|---|---|---|---|
| **Identificador único** | Sistema de Información de la Administración Universitaria (SIAUWEB) | | |
| **(Nombre del sistema A5)** | Sistema de Información de la Administración Universitaria (SIAUWEB) | | |
| **Actividad** | **Descripción** | **Duración** | **Cobertura** |
| Actualización del sistema operativo. | Se hace uso de la herramienta de actualización de software de macos. | En promedio de 2 a 4 horas. | Eliminación de problemas de seguridad y vulnerabilidades del sistema operativo. |
| Actualización del cliente FTP. | Se hace uso de la herramienta integrada en el sistema (*check update*). | Aproximadamente de 2 a 3 horas. | Solucionar errores de conexión SSH. |

| | | | |
|---|---|---|---|
| Renovación de Certificado de seguridad | Proceso de renovación con el Departamento Coordinación de Servicios de Identidad y Firma Electrónica Universitaria de la DGTIC. | 5 días hábiles. | Anualmente |

### 8.2 Actualización y mantenimiento de equipo de cómputo

| **Departamento del área de Sistemas** | | | |
|---|---|---|---|
| **Identificador único** | PUDH-WEB | | |
| **(Nombre del sistema A1)** | www.pudh.unam.mx | | |
| **Actividad** | **Descripción** | **Duración** | **Cobertura** |
| Mantenimiento preventivo y correctivo. | Realizar acciones de revisión, limpieza o reparación para garantizar el buen funcionamiento y fiabilidad. | De manera semestral. | Se reduce el mínimo, riesgo de pérdida de datos por fallas en el equipo. |
| Renovación de equipo de cómputo | Solicitud de asignación de nuevo equipo de cómputo. | Cinco meses. | Convocatoria anual. |

| **Archivo General del PUDH** | | | |
|---|---|---|---|
| **Identificador único** | PUDH-AGP | | |
| **(Nombre del sistema A2)** | Archivo General del PUDH | | |
| **Actividad** | **Descripción** | **Duración** | **Cobertura** |
| Mantenimiento preventivo y correctivo. | Realizar acciones de revisión, limpieza o reparación para garantizar el buen funcionamiento y fiabilidad. | De manera semestral. | Se reduce el mínimo, riesgo de pérdida de datos por fallas en el equipo. |
| Renovación de equipo de cómputo | Solicitud de asignación de nuevo equipo de cómputo. | Cinco meses. | Convocatoria anual. |

| **Delegación Administrativa** | | | |
|---|---|---|---|
| **Identificador único** | SISTEMA INSTITUCIONAL DE PERSONAL (SIP) | | |
| **(Nombre del sistema A3)** | SISTEMA INSTITUCIONAL DE PERSONAL (SIP) | | |
| **Actividad** | **Descripción** | **Duración** | **Cobertura** |
| Mantenimiento preventivo y correctivo. | Realizar acciones de revisión, limpieza o reparación para garantizar el buen | De manera semestral. | Se reduce el mínimo, riesgo de pérdida de datos por fallas en el equipo. |

| | | | |
|---|---|---|---|
| | funcionamiento y fiabilidad. | | |
| Renovación de equipo de cómputo | Solicitud de asignación de nuevo equipo de cómputo. | Cinco meses. | Convocatoria anual. |

| **Delegación Administrativa** | | | |
|---|---|---|---|
| **Identificador único** | SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI) | | |
| **(Nombre del sistema A4)** | SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI) | | |
| **Actividad** | **Descripción** | **Duración** | **Cobertura** |
| Mantenimiento preventivo y correctivo. | Realizar acciones de revisión, limpieza o reparación para garantizar el buen funcionamiento y fiabilidad. | De manera semestral. | Se reduce el mínimo, riesgo de pérdida de datos por fallas en el equipo. |
| Renovación de equipo de cómputo | Solicitud de asignación de nuevo equipo de cómputo. | Cinco meses. | Convocatoria anual. |

| **Delegación Administrativa** | |
|---|---|
| **Identificador único** | Sistema de Información de la Administración Universitaria (SIAUWEB) |

| | | | |
|---|---|---|---|
| | | | |
| **(Nombre del sistema A5)** | Sistema de Información de la Administración Universitaria (SIAUWEB) | | |
| **Actividad** | **Descripción** | **Duración** | **Cobertura** |
| Mantenimiento preventivo y correctivo. | Realizar acciones de revisión, limpieza o reparación para garantizar el buen funcionamiento y fiabilidad. | De manera semestral. | Se reduce el mínimo, riesgo de pérdida de datos por fallas en el equipo. |
| Renovación de equipo de cómputo | Solicitud de asignación de nuevo equipo de cómputo. | Cinco meses. | Convocatoria anual. |

### 8.3 Procesos para la conservación, preservación y respaldos de información

| **Departamento del área de sistemas** | | |
|---|---|---|
| **Identificador único** | PUDH-WEB | |
| **(Nombre del sistema A1)** | *www.pudh.unam.mx* | |
| **Proceso** | **Descripción** | **Responsable** |
| Respaldo de equipo principal. | Se realiza el volcado de la base de datos del servidor, se genera un archivo el | Octavio Beltrán Estévez. |

| | | |
|---|---|---|
| | cual se almacena en un dispositivo externo.<br><br>Cada respaldo se almacena durante un periodo de tiempo indefinido<br><br>Periodicidad semestral. | Tiempo máximo de ejecución: 1 día. |
| Conservación y protección de la información | Verificar el cifrado en cada uno de los respaldos que se almacenen en formato ZIP equivalente a AES de 128 bits<br><br>Periodicidad semestral. | Octavio Beltrán Estévez.<br>Tiempo máximo de ejecución: 1 día. |

| **Archivo General del PUDH** | | |
|---|---|---|
| **Identificador único** | PUDH-AGP | |
| **(Nombre del sistema A2)** | Archivo General del PUDH | |
| **Proceso** | **Descripción** | **Responsable** |
| Respaldo de hoja de cálculo. | Se realiza el respaldo de acuerdo a su criticidad. Se almacena en una unidad externa por tiempo indefinido. | Octavio Beltrán Estévez.<br>Tiempo máximo de ejecución: 1 día. |
| Conservación y protección de la información | Verificar el cifrado en cada uno de los respaldos que se almacenen en formato | Octavio Beltrán Estévez.<br>Tiempo máximo de ejecución: 1 día. |

| | | |
|---|---|---|
| | ZIP equivalente a AES de 128 bits<br><br>Periodicidad semestral. | |

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

| **Departamento del área de sistemas** | | |
|---|---|---|
| **Identificador único** | PUDH-WEB | |
| **(Nombre del sistema A1)** | *www.pudh.unam.mx* | |
| **Proceso** | **Descripción** | **Responsable** |
| Borrado de información en servidores. | Eliminación segura de datos almacenados, es fundamental para proteger la confidencialidad de la información. | Octavio Beltrán Estévez. |
| Formateo a bajo nivel. | Se efectúa el formateo de los discos duros que son sustituidos en cada equipo. Tomando en consideración el tamaño de la unidad dependerá el tiempo que tarde su ejecución. | Octavio Beltrán Estévez. |
| Ejecutar herramientas para borrado seguro | Sobrescribir los datos existentes con patrones aleatorios o ceros, | Centro de datos de la DGTIC |

| | | |
|---|---|---|
| | haciendo imposible la reconstrucción de los archivos utilizando el comando sswap | |

| **Archivo General del PUDH** | | |
|---|---|---|
| **Identificador único** | PUDH-AGP | |
| **(Nombre del sistema A2)** | Archivo General del PUDH | |
| **Proceso** | **Descripción** | **Responsable** |
| Borrado de información en equipos locales: contraseñas, accesos a sistemas de información, acceso a páginas personales, archivos o documentos innecesarios que consumen espacio o recursos de almacenamiento, entre otros. | Eliminación segura de datos almacenados es fundamental para proteger la confidencialidad de la información y la operación de los equipos. | Octavio Beltrán Estévez. |
| Formateo a bajo nivel. | Se efectúa el formateo de los discos duros que son sustituidos en cada equipo. | Octavio Beltrán Estévez.<br><br>Analizando el tamaño de la unidad dependerá el tiempo que tarde su ejecución. |
| Ejecutar herramientas para borrado seguro | Sobrescribir los datos existentes con patrones aleatorios o ceros, | Octavio Beltrán Estevéz |

| | | |
|---|---|---|
| | haciendo imposible la reconstrucción de los archivos utilizando el comando shred. | |

| **Delegación Administrativa** | | |
|---|---|---|
| **Identificador único** | *SISTEMA INTEGRAL DE PERSONAL (SIP)* | |
| **(Nombre del sistema A3)** | *SISTEMA INTEGRAL DE PERSONAL (SIP)* | |
| **Proceso** | **Descripción** | **Responsable** |
| NO APLICA | NO APLICA | NO APLICA |

| **Delegación Administrativa** | | |
|---|---|---|
| **Identificador único** | *SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI)* | |
| **(Nombre del sistema A4)** | *SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI)* | |
| **Proceso** | **Descripción** | **Responsable** |
| NO APLICA | NO APLICA | NO APLICA |

| **Delegación Administrativa** | |
|---|---|
| **Identificador único** | Sistema de Información de la Administración Universitaria (SIAUWEB) |

| | | |
|---|---|---|
| | | |
| **(Nombre del sistema A5)** | Sistema de Información de la Administración Universitaria (SIAUWEB) | |
| **Proceso** | **Descripción** | **Responsable** |
| NO APLICA | NO APLICA | NO APLICA |

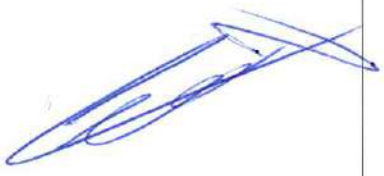
## 9. Procedimiento para la cancelación de datos personales

Para la cancelación de datos personales como parte de la garantía de los derechos ARCO, El PUDH-UNAM se encuentra trabajando en la implementación de procedimientos adecuados para la cancelación de datos y está en la mejor disposición de realizar cualquier acción para poder llevar cualquier requerimiento que le sea solicitado.

| **Programa Universitario de Derechos Humanos** | |
|---|---|
| **Identificador único** | PUDH-WEB |
| **(Nombre del sistema A1)** | *www.pudh.unam.mx* |
| **Identificador único** | PUDH-AGP |
| **(Nombre del sistema A2)** | Archivo General del PUDH |
| **Identificador único** | *SISTEMA INTEGRAL DE PERSONAL (SIP)* |
| **(Nombre del sistema A3)** | *SISTEMA INTEGRAL DE PERSONAL (SIP)* |
| **Identificador único** | *SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI)* |
| **(Nombre del sistema A4)** | *SISTEMA ADMINISTRATIVO INSTITUCIONAL (SAI)* |
| **Identificador único** | Sistema de Información de la Administración Universitaria (SIAUWEB) |
| **(Nombre del sistema A5)** | Sistema de Información de la Administración Universitaria (SIAUWEB) |

| **Procedimiento para la cancelación de datos** |
| --- |
| La cancelación de datos personales se desarrolla en los siguientes etapas:<br><br>1. Identificar los datos personales que serán cancelados, una vez que han dejado de ser necesarios para las labores del Programa o cuando se haya recibido una solicitud para la cancelación de los mismos; se eliminarán todos los registros y copias de seguridad.<br><br>2. Notificar a los titulares de los datos personales sobre la cancelación del sistema de tratamiento de datos.<br><br>3. Eliminar los datos personales de manera segura, utilizando procedimientos de borrado seguro que impidan la recuperación en las bases de datos y todos sus respaldos.<br><br>4. Verificar que los datos hayan sido eliminados correctamente y que no queden copias después del proceso.<br><br>5. Documentar todo el proceso de cancelación, incluyendo la fecha y hora de la eliminación, el método utilizado y la verificación de la eliminación de los datos. |

## Aprobación del Documento de Seguridad

| | | **Nombre y firma de quienes revisaron el presente documento:** |
|---|---|---|
| **Responsable del desarrollo:** | José Luis Belmont Lugo<br>Secretario Técnico<br>*pudhsec_tecnica@unam.mx* | |
| **Revisó:** | Noemi Monroy Enriquez<br>Secretaria Académica<br>*noemi.monroy@unam.mx*<br>Abigail Leyva Martínez<br>Jefa de Clínica Jurídica<br>*pudh_cj_dir@unam.mx*<br>Yadira Alicia Gallardo Guillén<br>Delegada Administrativa<br>*ygallardog@unam.mx*<br>Octavio Beltrán Estévez<br>Asistente de Procesos<br>*obeltran@unam.mx* | |
| **Autorizó:** | Alfredo Sánchez Castañeda<br>Coordinador del Programa Universitario de Derechos Humanos<br>*pudh_coordinacion@unam.mx* |  |
| **Fecha de emisión:** | 14 de octubre de 2026 | |