



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Documento de Seguridad

DDUIAVG-SGSDP-DS

Tabla de autorización

Elaboración

Ing. Héctor Javier Correa Peragallo

Tel: 5556 226109, hcorrea@defensoria.unam.mx

Jefe de Sistemas

Revisión

Mtro. César Flores Mancilla

Tel: 5556 226225, cflores@defensoria.unam.mx

Responsable de Seguridad de Datos Personales

Aprobación

Dra. Guadalupe Barrena Nájera

Tel: 5556 226222, guadalupe@defensoria.unam.mx

Titular de la Defensoría de los Derechos Universitarios,



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Igualdad y Atención de la Violencia de Género

Sistema de Gestión de Seguridad de Datos Personales

Documento de Seguridad

Índice

Introducción	7
A. Sistema de Gestión	8
1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES	8
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES	22
3. ANÁLISIS DE RIESGOS	22
4. ANÁLISIS DE BRECHA	23
5. PLAN DE TRABAJO	25
6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS	26
I. TRANSFERENCIAS DE DATOS PERSONALES	26
II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	27
III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA:	31
IV. REGISTRO DE INCIDENTES:	31
V. ACCESO A LAS INSTALACIONES	31
VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES	32
VII. PERFILES DE USUARIO Y CONTRASEÑAS	32
VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS	33
IX. PLAN DE CONTINGENCIA	34
7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD	34
7.1 Herramientas y recursos para monitoreo de la protección de datos personales	34
7.2 Procedimiento para la revisión de las medidas de seguridad	34
7.3 Resultados de la evaluación y pruebas a las medidas de seguridad	35



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

7.4 Acciones para la corrección y actualización de las medidas de seguridad	35
8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN	35
8.1 Programa de capacitación a los responsables de tratamiento de datos personales	35
8.2 Programa de difusión de la protección a los datos personales	36
9. MEJORA CONTINUA	36
9.1 Actualización y mantenimiento de sistemas de información	36
9.2 Actualización y mantenimiento de equipo de cómputo	37
9.3 Procesos para la conservación, preservación y respaldos de información	37
9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos	37
10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES	38
B. Sistema de Control de Acceso	40
1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES	40
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES	41
3. ANÁLISIS DE RIESGOS	41
4. ANÁLISIS DE BRECHA	42
5. PLAN DE TRABAJO	42
6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS	42
I. TRANSFERENCIAS DE DATOS PERSONALES	42
II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	43
III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA	43
IV. REGISTRO DE INCIDENTES	43
V. ACCESO A LAS INSTALACIONES	44
VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES	44
VII. PERFILES DE USUARIO Y CONTRASEÑAS	45
VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS	45
IX. PLAN DE CONTINGENCIA	46
7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD	46
7.1 Herramientas y recursos para monitoreo de la protección de datos personales	46
7.3 Resultados de la evaluación y pruebas a las medidas de seguridad	46



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

7.4 Acciones para la corrección y actualización de las medidas de seguridad	47
8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN	47
8.1 Programa de capacitación a los responsables de tratamiento de datos personales	47
8.2 PROGRAMA DE DIFUSIÓN DE LA PROTECCIÓN A LOS DATOS PERSONALES	48
9. MEJORA CONTINUA	48
9.1 Actualización y mantenimiento de sistemas de información	48
9.2 Actualización y mantenimiento de equipo de cómputo	48
9.3 Procesos para la conservación, preservación y respaldos de información	49
9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos	49
10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES	49
C. Sistema de Video Vigilancia	51
I. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES	51
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES	51
3. ANÁLISIS DE RIESGOS	52
4. ANÁLISIS DE BRECHA	52
5. PLAN DE TRABAJO	52
6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS	53
I. TRANSFERENCIAS DE DATOS PERSONALES	53
II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICO	53
III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA	53
IV. REGISTRO DE INCIDENTES	54
V. ACCESO A LAS INSTALACIONES	54
VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES	55
VII. PERFILES DE USUARIO Y CONTRASEÑAS	55
VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS	55
IX. PLAN DE CONTINGENCIA	56
7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD	56
7.1 Herramientas y recursos para monitoreo de la protección de datos personales	56
7.3 Resultados de la evaluación y pruebas a las medidas de seguridad	57



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

7.4 Acciones para la corrección y actualización de las medidas de seguridad	57
8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN	57
8.1 Programa de capacitación a los responsables de tratamiento de datos personales	57
8.2 Programa de difusión de la protección a los datos personales	58
9. MEJORA CONTINUA	58
9.1 Actualización y mantenimiento de sistemas de información	58
9.2 Actualización y mantenimiento de equipo de cómputo	58
9.3 Procesos para la conservación, preservación y respaldos de información	59
9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos	59
10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES	59
D. Sistema Integral de Personal	60
1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES	60
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES	61
3. ANÁLISIS DE RIESGOS	61
4. ANÁLISIS DE BRECHA	62
5. PLAN DE TRABAJO	62
6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS	62
I. TRANSFERENCIAS DE DATOS PERSONALES	62
ii. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	63
III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA	63
IV. REGISTRO DE INCIDENTES	63
V. ACCESO A LAS INSTALACIONES	63
VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES	64
VII. PERFILES DE USUARIO Y CONTRASEÑAS	64
VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS	65
IX. PLAN DE CONTINGENCIA	65
7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD	66
7.1 Herramientas y recursos para monitoreo de la protección de datos personales	66
7.3 Resultados de la evaluación y pruebas a las medidas de seguridad	66



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

7.4 Acciones para la corrección y actualización de las medidas de seguridad	66
8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN	67
8.1 Programa de capacitación a los responsables de tratamiento de datos personales	67
8.2 Programa de difusión de la protección a los datos personales	67
9. MEJORA CONTINUA	68
9.1 Actualización y mantenimiento de sistemas de información	68
9.2 Actualización y mantenimiento de equipo de cómputo	68
9.3 Procesos para la conservación, preservación y respaldos de información	68
9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos	69
10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES	69
E. Sistema Institucional de Compras	70
1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES	70
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES	71
3. ANÁLISIS DE RIESGOS	71
4. ANÁLISIS DE BRECHA	72
5. PLAN DE TRABAJO	72
6. Medidas de seguridad implementadas	73
I. TRANSFERENCIAS DE DATOS PERSONALES	73
II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	73
III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA:	75
IV. REGISTRO DE INCIDENTES	75
V. ACCESO A LAS INSTALACIONES	75
VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES	76
VII. PERFILES DE USUARIO Y CONTRASEÑAS	76
VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS	77
IX. PLAN DE CONTINGENCIA	77
7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD	77
7.1 Herramientas y recursos para monitoreo de la protección de datos personales	77
7.3 Resultados de la evaluación y pruebas a las medidas de seguridad	78



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

7.4 Acciones para la corrección y actualización de las medidas de seguridad	78
8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN	78
8.1 Programa de capacitación a los responsables de tratamiento de datos personales	78
8.2 Programa de difusión de la protección a los datos personales	79
9. MEJORA CONTINUA	79
9.1 Actualización y mantenimiento de sistemas de información	79
9.2 Actualización y mantenimiento de equipo de cómputo	80
9.3 Procesos para la conservación, preservación y respaldos de información	80
9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos	80
10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES	80
Aprobación del documento de seguridad	82



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Introducción

El presente documento de seguridad contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales de la esta área universitaria con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Su propósito es identificar los sistemas de tratamiento de datos personales que posee esta área universitaria, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

Este modelo pretende brindar a las áreas universitarias homogeneidad en la redacción, organización y contenido para que elaboren su propio documento de seguridad en el que se describan las tres medidas de seguridad para la protección de los datos personales.

El marco jurídico del documento de seguridad se regula por el capítulo II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada el 26 de enero de 2017, que establece un conjunto mínimo de medidas de seguridad que cada dependencia o entidad universitaria deberá considerar al perfilar su estrategia de seguridad para la protección de los datos personales bajo su custodia, según el tipo de soportes —físicos, electrónicos o ambos— en los que residen dichos datos y dependiendo del nivel de protección que tales datos requieran.

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

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



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

A. Sistema de Gestión

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Departamento de Sistemas	
Identificador único	<u>SDU1</u>
Nombre del Sistema	<u>Sistema de Gestión</u>
Datos personales (sensibles o no) contenidos en el sistema:	Datos de identificación: • Nombre • Domicilio • Teléfono particular • Teléfono celular • Correo electrónico • Fecha de nacimiento • CURP • Edad • Sexo • Género • Identificación con grupo minoritario
Encargados	
Nombre	Guadalupe Barrena Nájera
Cargo:	Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género
Funciones:	Coordinar y dar seguimiento a las actividades relacionadas con el sistema en cuanto al trámite de asuntos (orientaciones y quejas) por derechos universitarios y violencia de género.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre	Elizabeth Ayesha Borja Domínguez
Cargo:	Secretaria Auxiliar
Funciones:	Coadyuvar con la titular en coordinar y supervisar las actividades relacionadas con el sistema en cuanto al trámite de asuntos (orientaciones y quejas) por violencia de género.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Nombre	César Flores Mancilla
Cargo:	Secretario Auxiliar
Funciones:	Coadyuvar con la titular en coordinar y supervisar las actividades relacionadas con el sistema en cuanto al trámite de asuntos (orientaciones y quejas) por derechos universitarios.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre	Miriam Camacho Valladares
Cargo:	Coordinadora del Área de Psicología
Funciones:	Coadyuvar con la titular en coordinar y supervisar las actividades relacionadas con el sistema en cuanto al apoyo que brinda el personal de psicología en el trámite de asuntos (orientaciones y quejas).
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre	Mara Hernández Estrada
Cargo:	Responsable del Área de Procedimiento Alternativo
Funciones:	Coadyuvar con la titular en coordinar y supervisar las actividades relacionadas con el sistema en cuanto al trámite de procedimientos alternativos.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre	Leticia Escamilla Ruiz
Cargo:	Responsable del Área de Primer Contacto
Funciones:	Coadyuvar con la titular en coordinar y supervisar las actividades relacionadas con el sistema en cuanto al apoyo que brinda el Área de Primer Contacto.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Responsable	



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Nombre:	Héctor Javier Correa Peragallo
Cargo:	Jefe de Departamento
Funciones:	Realización de adecuaciones al sistema y su base de datos, actualización de los catálogos de las bases de datos según sea requerido, administración de usuarios, configuración de perfiles de acceso al sistema y base de datos. Elaboración de los reportes y estadísticas solicitadas para la elaboración de informes y respuestas a solicitudes de información.
Obligaciones:	Monitorear el funcionamiento y manejo de la información relativa a la atención de casos, turnos y correos electrónicos registrados a través del sistema. Adoptar las medidas necesarias para asegurar el correcto funcionamiento y disponibilidad del sistema y los registros almacenados. Realizar las adecuaciones técnicas necesarias al sistema conforme a las solicitudes realizadas por los funcionarios de la dependencia. Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Usuarios	
Nombre del Usuario 1	Adela Noemi Monroy Enriquez
Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 2	Luis Eduardo Huerta Velázquez
Cargo:	Jefe de Departamento
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 3	Alejandra Arenas Nava



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 4	Julio Cesar Laydes Villegas
Cargo:	Abogado Auxiliar
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 5	Mónica Yeraldi Ortiz Galindo
Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 6	Alejandra Álvarez Huerta
Cargo:	Abogada Auxiliar
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 7	Mario Alberto Gómora Gálvez
Cargo:	Asistente Ejecutivo
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 8	Diego Iván Huitrón González



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Cargo:	Abogado auxiliar
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 9	Gabriela Martínez Pérez
Cargo:	Abogada Asesora
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 10	Aditi Oropeza Martínez
Cargo:	Abogada
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 11	Delia Beatriz García Valencia
Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 12	Gisela Cárdenas Delgado
Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 13	Ana Bertha Cervantes Troop



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 14	Samantha Rivera Flores
Cargo:	Jefa de Unidad
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 15	Gabriela Rodríguez Rojas
Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 16	Gisel Mateos González
Cargo:	Abogada
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 17	Heradia Elizabeth Ordoñez Quinto
Cargo:	Jefa de Unidad
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 18	Leticia Domínguez Bautista



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 19	Beatriz Angélica Jiménez Santillán
Cargo:	Abogada
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 20	Graciela Maribel Cervantes Guerra
Cargo:	Abogada
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 21	Patricia Ibarra Tapia
Cargo:	Jefa de Unidad
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 22	Gabriela Torres de la Paz
Cargo:	Jefa de Unidad
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 23	Josari Fernanda Mendoza Vázquez



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Cargo:	Abogada
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 24	Lizeth Fuentes Reyes
Cargo:	Abogada
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 25	María del Sacramento Díaz Domínguez
Cargo:	Abogada
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 26	Mitzi Gabriela Alvarado Feregrino
Cargo:	Abogada
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 27	Nubia Araceli Nava Gama
Cargo:	Abogada
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 28	Ortencia Trejo Ruiz



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Cargo:	Abogada
Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 29	Concepción García Márquez
Cargo:	Asistente Ejecutivo
Funciones:	Participar en la correcta alimentación de las bases de datos que permitan el control de los procesos que se efectúen en la Defensoría.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 30	Rosa Elena Carrera Victorino
Cargo:	Asistente de Procesos
Funciones:	Alimentar y mantener actualizados los registros en el sistema de acuerdo que permitan el control de los procesos que se efectúen en la Defensoría.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 31	Minerva Hernández Virgen
Cargo:	Asistente Ejecutivo
Funciones:	Participar en la correcta alimentación de las bases de datos que permitan el control de los procesos que se efectúen en la Defensoría.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 32	María Concepción Capulín Arellano
Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 33	Nallely Paredes Ruiz
Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 34	Diana Laura Antonio Martínez
Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 35	Ana Gabriela García Fernández
Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 36	Alma Saraí Villegas Moreno
Cargo:	Psicóloga
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 37	Valeria Mata Alcibar



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 38	Alma Delia Luis Reyes
Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 39	María Esther Rodríguez Dionicio
Cargo:	Psicóloga
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 40	Cecilia Espitia Carrasco
Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 41	Alma Denisse Ibáñez Rangel
Cargo:	Psicóloga
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 42	Ana Karen Gutiérrez Zendejas
Cargo:	Psicóloga
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 43	Araceli Gutiérrez Ramírez
Cargo:	Psicóloga
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 44	Karen Díaz Hernández
Cargo:	Psicóloga
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 45	María de los Ángeles de Santiago Morales
Cargo:	Psicóloga
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 46	Perla Paola Santiago Nava



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Cargo:	Psicóloga
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 47	Susan Correa Salazar
Cargo:	Psicóloga
Funciones:	Alimentar y mantener actualizados los registros en el sistema de información respecto del apoyo psicológico proporcionado a la comunidad universitaria.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 48	Natalia Alcántara Manríquez
Cargo:	Trabajadora Social
Funciones:	Alimentar y mantener actualizados los registros en el sistema respecto de la atención de primer contacto proporcionada a la comunidad universitaria en casos de violencia de género.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 49	Norma Raquel Moreno Ríos
Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros en el sistema respecto de la atención de primer contacto proporcionada a la comunidad universitaria en casos de violencia de género.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 50	Diana Abigail Salinas Garay
Cargo:	Jefa de Departamento
Funciones:	Alimentar y mantener actualizados los registros en el sistema respecto de la atención de primer contacto proporcionada a la comunidad universitaria en casos de violencia de género.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 51	Jennifer Isela Ramos Rodríguez
Cargo:	Trabajadora Social
Funciones:	Alimentar y mantener actualizados los registros en el sistema respecto de la atención de primer contacto proporcionada a la comunidad universitaria en casos de violencia de género.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 52	Patricia Bernal Ginez
Cargo:	Trabajadora Social
Funciones:	Alimentar y mantener actualizados los registros en el sistema respecto de la atención de primer contacto proporcionada a la comunidad universitaria en casos de violencia de género.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 53	Julia Elena Santiago Velasco
Cargo:	Jefa de la Unidad Administrativa
Funciones:	Alimentar el sistema para el registro de número de oficio de la Unidad Administrativa.
Obligaciones:	Guardar la confidencialidad de la información relativa a los oficios registrados, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 54	Adolfo Rosalio Serrano
Cargo:	Asistente de Procesos
Funciones:	Coadyuvar con el jefe del Departamento de Sistemas en la correcta alimentación de las bases de datos que permitan el control de los procesos que se efectúen en la Defensoría.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre del Usuario 55	Ixchel Rosario Molotla Santoyo
Cargo:	Abogada Auxiliar



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Funciones:	Alimentar y mantener actualizados los registros respecto al trámite de orientaciones y quejas.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.

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

Departamento de Sistemas	
Identificador único:	<u>SDU1</u>
Nombre del sistema:	<u>Sistema de Gestión</u>
Tipo de soporte:	El sistema se encuentra en soporte físico y electrónico.
Descripción:	Los soportes físicos se encuentran en expedientes y los electrónicos se encuentran en base de datos y archivos electrónicos.
Características del lugar donde se resguardan los soportes:	El soporte físico se encuentra almacenado en el archivo de concentración, que es una oficina bajo llave, con una dimensión de 9.51 metros cuadrados, conteniendo la información en archiveros. El archivo de concentración se encuentra dentro de las instalaciones centrales de la Defensoría, a la cual se tiene acceso mediante un control biométrico. Los soportes electrónicos se encuentran en una máquina virtual del Centro de Datos de la UNAM, el cual cuenta con controles de acceso, respaldo de energía por UPS y planta de respaldo.

3. ANÁLISIS DE RIESGOS

Información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

[illegible]

4. ANÁLISIS DE BRECHA

Información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

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



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

[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]



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

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

5. PLAN DE TRABAJO

Información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

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



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

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



Defensoría de los
Derechos Universitarios
Igualdad y Atención de
la Violencia de Género

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género	
Identificador único	<u>SDU1</u>
Nombre del sistema	<u>Sistema de Gestión</u>
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos	El envío de información en soportes físicos se lleva a cabo a través de una persona designada como mensajero. Los documentos se guardan en un sobre con membrete debidamente cerrado, de forma que es perceptible cualquier violación antes de su entrega. Al llegar al destino en donde se realizará la entrega, el mensajero constata que sea el domicilio y dependencia a la que va dirigida la comunicación, además de que se verifica con la persona que se encuentre en la recepción de que es el lugar correcto para recibir la comunicación. La persona que recibe la comunicación constata que su dependencia es la destinataria, procediendo a plasmar en el acuse correspondiente el sello de la entidad receptora, además de colocar su nombre, rúbrica, fecha y hora, dando cuenta de la recepción.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

	Una vez que se tiene el acuse de recibo, el mensajero lo entrega a personal del área de la Defensoría, según corresponda, a efecto de hacer el registro correspondiente en las bitácoras del Sistema de Gestión.
Transferencias mediante el traslado de soportes electrónicos	El envío de información en soportes electrónicos se realiza mediante una persona designada como mensajero. Los documentos electrónicos enviados a través de dispositivos de almacenamiento (CD, USB, entre otros) se guardan en un sobre con membrete debidamente cerrado, de forma que es perceptible cualquier violación antes de su entrega. Al llegar al destino en donde se realizará la entrega, el mensajero constata que sea el domicilio y dependencia a la que va dirigida la comunicación, además de que se verifica con la persona que se encuentre en la recepción de que es el lugar correcto para recibir la comunicación. La persona que recibe la comunicación constata que su dependencia es la destinataria, procediendo a plasmar en el acuse correspondiente el sello de la entidad receptora, además de colocar su nombre, rúbrica, fecha y hora, dando cuenta de la recepción. Una vez que se tiene el acuse de recibo, el mensajero lo entrega a personal del área de la Defensoría, según corresponda, a efecto de hacer el registro correspondiente en las bitácoras del Sistema de Gestión.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Transferencias mediante el traslado sobre redes electrónicas

El envío de información mediante redes electrónicas se realiza a través de oficios firmados electrónicamente y enviados como archivo adjunto a través del correo electrónico institucional, el cual es administrado por la UNAM el cual cuenta con protección anti malware y con un canal de comunicación seguro SSL que cifra la información.

En las comunicaciones Regularmente las autoridades universitarias destinatarias de las comunicaciones confirman la recepción de la información a través del mismo medio.

Cada envío de información que se hace se registra en las bitácoras del Sistema de Gestión.

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

1. Medidas de seguridad implementadas para el resguardo de los soportes físicos del sistema:

Los soportes físicos del Sistema constan en expedientes impresos de los casos atendidos en esta Defensoría, que se encuentra en carpetas físicas con un número de control interno y que se almacenan –de acuerdo al área de atención– en los estantes del Archivo de Concentración, el cual se encuentra ubicado en las instalaciones de la oficina central de la Defensoría y cuenta con cerradura para mantener el control de entrada del personal usuario.

Asimismo, cabe mencionar que a las instalaciones de la Defensoría se accede mediante control biométrico, mismo que está conectado a un UPS, además de que se cuenta con cámaras de video vigilancia.

2. Listado de persona que tienen acceso a los soportes físicos del sistema:

Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género
--



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Identificador único	<u>SDU1</u>
Nombre del Sistema	<u>Sistema de Gestión</u>
Responsable	
Nombre:	Julia Elena Santiago Velasco
Cargo:	Jefa de la Unidad Administrativa
Funciones:	Administrar los recursos financieros, humanos, materiales y servicios con que cuenta la dependencia, para su desarrollo y funcionamiento, dando apoyo a las áreas de la Defensoría y alcanzar las metas encomendadas.
Obligaciones:	Supervisar los procesos relacionados con la administración en el cambio de la situación laboral del personal administrativo de base, confianza y funcionario. Rendir informes periódicos del estado que guarda la Defensoría de los Derechos Universitarios y de los asuntos encomendados por el Titular. Guardar la confidencialidad de la información relativa los datos biométricos, haciendo uso exclusivo para los fines que hayan sido recabados.
Personal autorizado	
Nombre	Guadalupe Barrena Nájera
Cargo:	Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género
Funciones:	Coordina el trámite de los asuntos por violencia de género y derechos universitarios, y suscribe los oficios, acuerdos y recomendaciones para su determinación. Coordinar la administración y distribución correcta de los recursos humanos, materiales, tecnológicos y financieros, asignados al área para el cumplimiento de las actividades encomendadas. Mantener comunicación con las distintas autoridades universitarias internas y externas para tratar asuntos materia de su competencia. Supervisar y vigilar que los sistemas de control se lleven a cabo, a efecto de conocer permanentemente el avance de los asuntos competencia de la Dirección. Coordinar, promover y vigilar el desarrollo de los programas sustantivos y de gestión interna, a efecto de propiciar los conceptos de mejora continua y calidad total, en cumplimiento



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

	a los lineamientos, políticas, contratos colectivos de trabajo y normatividad vigentes en la UNAM, en materia de administración de personal. Establecer normas, políticas, procedimientos y programas internos que promuevan y controlen las actividades que se desarrollan en la Dependencia.
Nombre	Elizabeth Ayesha Borja Domínguez
Cargo:	Secretaria Auxiliar
Funciones:	Coadyuvar con la titular en la vigilancia del cumplimiento del orden legal universitario, cuando los legitimados para acudir a la Defensoría soliciten su intervención o de oficio cuando así proceda, así como en el desarrollo de las actividades que dentro de su competencia corresponden a este Órgano Universitario.
Obligaciones:	Recibir quejas por violencia de género y tramitar el procedimiento conforme la Legislación Universitaria. Brindar orientación y apoyo legal y psicológico. Vigilar que las labores dentro de su ámbito de competencia se desarrollen ordenada y eficientemente. Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre	César Flores Mancilla
Cargo:	Secretario Auxiliar
Funciones:	Coadyuvar con la titular en la vigilancia del cumplimiento del orden legal universitario, cuando los legitimados para acudir a la Defensoría soliciten su intervención o de oficio cuando así proceda, así como en el desarrollo de las actividades que dentro de su competencia corresponden a este Órgano Universitario.
Obligaciones:	Recibir quejas por violaciones a derechos universitarios y tramitar el procedimiento conforme la Legislación Universitaria. Brindar orientación jurídica y apoyo psicológico. Vigilar que las labores dentro de su ámbito de competencia se desarrollen ordenada y eficientemente. Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Nombre	Alejandra Arenas Nava
Cargo:	Jefa de Departamento
Funciones:	Proporcionar orientación a la comunidad universitaria, bajo la supervisión de los defensores adjuntos. Coadyuvar con los defensores adjuntos en el trámite de los asuntos y las quejas.
Obligaciones:	Alimentar y mantener actualizados los registros en los sistemas de información de acuerdo con las labores del cargo que desempeña. Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre	Rosa Elena Carrera Victorino
Cargo:	Asistente de Procesos
Funciones:	Alimentar y mantener actualizados los registros en el sistema de acuerdo que permitan el control de los procesos que se efectúen en la Defensoría.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.
Nombre	Minerva Hernández Virgen
Cargo:	Asistente Ejecutivo
Funciones:	Participar en la correcta alimentación de las bases de datos que permitan el control de los procesos que se efectúen en la Defensoría.
Obligaciones:	Guardar la confidencialidad de la información relativa a los casos y atenciones brindadas, haciendo uso exclusivo para los fines que hayan sido recabados.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA:

El sistema cuenta con registros electrónicos de eventos de operación que se guardan en la base de datos hasta un año, almacenando el nombre de usuario, aplicación y página consultada, fecha, tiempo de sesión abierta, sesiones activas y dirección IP.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Para asegurar la integridad de las bitácoras, solamente el administrador del sistema tiene acceso a la base de datos, además de ser respaldados junto con el resto de los registros de la base de datos.

La bitácora es revisada aleatoriamente por el administrador del sistema. No se cuenta con herramienta para su análisis automático por lo que se realiza de manera manual.

IV. REGISTRO DE INCIDENTES:

Se establecerán registros de incidentes tanto de los soportes físicos o electrónicos, en los que se debe contemplar:

- a) Nombre de la persona que gestionó el incidente
- b) Fecha, hora y lugar del incidente
- c) Afectación y alcance del incidente
- d) Metodología aplicada
- e) Soportes físicos o electrónicos afectados

Para el caso de cualquier incidente, el responsable del sistema dará vista al titular del área universitaria para su conocimiento, así como al Responsable de Seguridad de Datos Personales, para que en el ámbito de sus atribuciones determinen lo conducente.

En el caso de robo o extravío de datos personales, se alertará a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior:

El edificio donde se encuentran las instalaciones cuenta con vigilancia las 24 horas, el control de acceso a la dependencia es mediante equipo biométrico, se cuenta con equipo de video vigilancia que resguarda los videos en el disco duro de un DVR.

Al tratarse de un área que brinda asistencia a la comunidad universitaria en general, las personas que acceden a las instalaciones:

- a) No tienen que identificarse
- b) La autenticación mediante huella es necesaria para el personal de la Defensoría



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

- c) En caso de personas ajenas a la Defensoría, se les da acceso a personas que solicitan atención para casos que este órgano universitario está facultado para atender.

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

Los soportes electrónicos se encuentran en el Centro de Datos de la UNAM, el cual cuenta con varios filtros de seguridad para el acceso, control mediante dispositivos biométricos para el acceso, puertas de seguridad en caso de toma de las instalaciones y equipo de video vigilancia.

Para los soportes físicos que se encuentran en el archivo de concentración, se cuenta con vigilancia 24 horas en el edificio.

Para las personas que acceden a dichos espacios interiores:

- a) Sólo tiene acceso el personal de la Defensoría
- b) El acceso se autoriza a solicitud del personal con acceso autorizado a los expedientes.

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

Cualquier rectificación de datos personales se deberá ceñir a los procedimientos institucionales consignados en la normatividad universitaria aplicable en la materia de protección de datos personales (Derechos ARCO).

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

- 1. El modelo de control de acceso para los equipos está basado en roles.
- 2. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
 - a) Tiene un manejo riguroso de perfiles de usuario y contraseña.
 - b) La contraseña de los usuarios se guarda de manera cifrada en la base de datos.
- 3. Administración de perfiles de usuario y contraseñas:



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

- a) El jefe del Departamento de Sistema da de alta los nuevos perfiles.
 - b) Esto se hace previa autorización de la titular.
 - c) En la base de datos se registra la fecha y cuenta que realizó la modificación.
- 4. Acceso remoto al sistema de tratamiento de datos personales:**
- a) Los usuarios del sistema de gestión requieren acceso remoto al mismo, ya que hay personal trabajando en sedes externas y por la naturaleza de los casos atendidos, en ocasiones es necesario el acceso a la información fuera de los horarios de oficina.
 - b) El administrador requiere acceso remoto al servidor de aplicaciones ya que es necesario para la solución de incidentes o consulta de información requerida en horarios fuera de oficina, debido a la naturaleza de los casos que se atiende.
 - c) El acceso remoto no autorizado al servidor de aplicaciones y base de datos está restringido por un certificado con llave primaria y contraseña segura.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Los respaldos se realizan de acuerdo con la política del Centro de Datos de la UNAM
 - a) Completo 1 y 1 incremental;
 - b) De forma automática,
 - c) Periodicidad con que los realiza: semanal
2. Se utiliza una máquina virtual como medio de almacenamiento.
3. Esta se ubica, de igual forma, en el Centro de Datos de la UNAM.
4. Los responsables de la realización de los respaldos, es el personal del Centro de Datos de la UNAM.

IX. PLAN DE CONTINGENCIA

La información contenida en la base de datos puede ser recuperada y restaurada para su operación mediante los respaldos que se realizan de manera automática en el Centro de Datos de la UNAM.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Se cuenta con un sitio alterno tibio en el antiguo edificio de posgrado con capacidad para hospedar parte del personal de la oficina central, restaurando la operación en un tiempo razonable.

El plan de contingencia se encuentra en desarrollo.

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

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

Departamento de Sistemas		
Identificador único	<u>SDU1</u>	
Nombre del sistema	<u>Sistema de Gestión</u>	
Recurso	Descripción	Control
Application Express	Revisiones aleatorias mediante la interfaz de administración	El jefe del Departamento de Sistema analiza los reportes de actividades dentro de la aplicación, con el fin de revisar comportamientos inusuales
Manejo de roles y permisos	Los permisos y privilegios se determinan mediante los roles asignados a las cuentas de los usuarios	El jefe del Departamento de Sistemas realiza la asignación de permisos y roles, conforme al diseño establecido para el sistema

7.2 Procedimiento para la revisión de las medidas de seguridad

Departamento de Sistemas	
Identificador único	<u>SDU1</u>
Nombre del sistema	<u>Sistema de Gestión</u>



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Medida de seguridad	Procedimiento	Responsable
Pruebas de penetración	Se realizaron pruebas de penetración por parte de la Dirección de Seguridad de DGTIC y se atendieron las observaciones derivadas de las pruebas	a) Ing. Héctor Javier Correa Peragallo b) 25 días en las pruebas y atención de observaciones

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

Departamento de Sistemas		
Identificador único	<u>SDU1</u>	
Nombre del sistema	<u>Sistema de Gestión</u>	
Medida de seguridad	Resultado de evaluación	Responsable
Implementación de protocolo HTTPS en servidor de aplicación	Es recomendable el uso de un canal cifrado de comunicación entre el cliente y el servidor de aplicación	a) Ing. Héctor Javier Correa Peragallo b) Noviembre de 2021

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

Departamento de Sistemas	
Identificador único	<u>SDU1</u>



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Nombre del sistema	Sistema de Gestión	
Medida de seguridad	Acciones	Responsable
Implementación de certificado SSL	Se adquirió e instaló el certificado SSL recomendado por la DGTIC. Dicho certificado será actualizado periódicamente para no perder su vigencia y protección.	a) Ing. Héctor Javier Correa Peragallo b) Diciembre de 2021.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Departamento de sistemas			
Identificador único	SDU1		
Nombre del sistema	Sistema de Gestión		
Actividad	Descripción	Duración	Cobertura
Curso Medidas de seguridad técnicas para la protección de datos personales	Curso en línea impartido por la DGTIC	Del 8 de febrero al 14 de marzo de 2021, con duración equivalente a 25 horas.	Personal del Departamento de Sistemas.
Programa de capacitación sobre protección de datos personales	Impartido en conjunto por la DGTIC y la Unidad de Transparencia	Del 22 al 25 de marzo, de 12 a 14:30	Personal involucrado en el desarrollo del documento de seguridad

8.2 Programa de difusión de la protección a los datos personales

Departamento de sistemas	
Identificador único	SDU1



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Nombre del sistema		<u>Sistema de Gestión</u>	
Actividad	Descripción	Duración	Cobertura
Difusión sobre seguridad informática	Sitio web con información sobre vulnerabilidades, riesgos, amenazas y buenas prácticas, el cual se difundió entre el personal	Sitio activo para difusión entre el personal de nuevo ingreso o que tiene acceso al sistema de gestión	Personal involucrado en el tratamiento de datos personales

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Departamento de sistemas			
Identificador único		<u>SDU1</u>	
Nombre del sistema		<u>Sistema de Gestión</u>	
Actividad	Descripción	Duración	Cobertura
Contrato de mantenimiento preventivo	Se realizó la contratación del mantenimiento preventivo del sistema	Dio inicio el 1 de agosto del 2022, renovándose a petición de la Defensoría	En caso de falla del sistema o su base de datos, se cuenta con el soporte técnico para su reparación

9.2 Actualización y mantenimiento de equipo de cómputo

Departamento de sistemas			
Identificador único		<u>SDU1</u>	
Nombre del sistema		<u>Sistema de Gestión</u>	
Actividad	Descripción	Duración	Cobertura
Ampliación de espacio de almacenamiento en máquina virtual	Se asignó el nuevo espacio asignado a la partición que usa el sistema para almacenamiento, asegurando contar con las condiciones necesarias para el	Cuatro horas, con inicio y fin el 29 de julio del 2021	El incremento en el almacenamiento le permite al sistema poder seguir operando de manera correcta por un periodo mínimo de dos años



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

	funcionamiento adecuado		
--	----------------------------	--	--

9.3 Procesos para la conservación, preservación y respaldos de información

Departamento de sistemas		
Identificador único	SDU1	
Nombre del sistema	Sistema de Gestión	
Proceso	Descripción	Responsable
Respaldo en línea	El Centro de Datos de la UNAM realiza 1 respaldo completo y 1 parcial cada semana	a) Administrador del Centro de Datos de la UNAM b) 1 día
Respaldo secundario	Se realiza un respaldo en almacenamiento secundario de la base de datos y aplicación	a) Ing. Héctor Javier Correa Peragallo b) 1 día

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

Departamento de sistemas	
Identificador único	SDU1



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Nombre del sistema	Sistema de Gestión	
	Proceso	Responsable
Borrado de disco duro	Cuando se cambia un disco duro de la máquina virtual, se solicita al Centro de Datos mediante oficio el borrado permanente de la información contenida.	Administrador del Centro de Datos de la UNAM 2 días

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

Cuando la totalidad de los datos personales contenidos en el Sistema de Gestión que hayan dejado de ser necesarios para el cumplimiento de la finalidad o finalidades para la que fueron recolectados, de conformidad con lo establecido en el Aviso de Privacidad o de acuerdo con las disposiciones legales aplicables, deberán ser cancelados previo bloqueo.

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

- Denominación: Sistema de Queja Virtual
- Motivo de la cancelación: Debido al desarrollo del Sistema de Gestión, el cual cumple con los requerimientos surgidos por la integración de las nuevas funciones de la Defensoría establecidas por el Consejo Universitario a partir del 14 de agosto del 2020.

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:¹

¹ Es el periodo por el que se conservará para efectos de responsabilidades, tomando en cuenta el plazo de su prescripción conforme la normatividad aplicable.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

El bloqueo del Sistema de Queja Virtual se realizará 5 días hábiles posteriores a la migración de los registros de orientaciones al Sistema de Gestión, contemplado en el Plan de Trabajo de este documento.

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

Para el bloqueo del Sistema de Queja Virtual, se deshabilitan los permisos de accesos a los usuarios con cualquier privilegio sobre la base de datos a nivel manejador de base de datos.

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

Una vez concluido el plazo para el bloqueo del Sistema de Queja Virtual, la supresión del sistema y los registros se hará de conformidad con el manual de procedimiento para el borrado seguro de la información de la Defensoría.



B. Sistema de Control de Acceso

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Identificador único:	<u>SDUCA</u>
Nombre del sistema:	<u>Sistema de Control de Acceso</u>
Datos personales contenidos en el sistema:	Datos de identificación: • Nombre • Fotografía • Datos biométricos de huella digital
Responsable	
Nombre:	Julia Elena Santiago Velasco
Cargo:	Jefa de la Unidad Administrativa
Funciones:	Dar seguimiento al sistema para la administración y supervisión de los recursos humanos, para su correcto desempeño.
Obligaciones:	Guardar la confidencialidad de la información relativa los datos biométricos, haciendo uso exclusivo para los fines que hayan sido recabados.
Encargado	
Nombre:	Héctor Javier Correa Peragallo
Cargo:	Jefe de Departamento
Funciones:	Administración de la base de datos, actualización de los registros de los equipos biométricos según sea requerido, administración de usuarios, configuración de perfiles de acceso a los equipos. Elaboración de los reportes y estadísticas solicitadas para la elaboración de informes.
Obligaciones:	Monitorear el funcionamiento y manejo de registros de los equipos biométricos de acceso. Adoptar las medidas necesarias para asegurar el correcto funcionamiento y disponibilidad de los registros almacenados.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

	Guardar la confidencialidad de la información relativa los datos biométricos, haciendo uso exclusivo para los fines que hayan sido recabados.
Usuarios	
Nombre:	Adolfo Rosalio Serrano
Cargo:	Asistente de Procesos
Funciones:	Coadyuvar con el jefe del Departamento de Sistemas en la correcta alimentación de los registros de control de acceso.
Obligaciones:	Guardar la confidencialidad de la información relativa los datos biométricos, haciendo uso exclusivo para los fines que hayan sido recabados.

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

Departamento de Sistemas	
Identificado único:	<u>SDUCA</u>
Nombre del sistema:	<u>Sistema de Control de Acceso</u>
Tipo de soporte:	El sistema se encuentra en soporte electrónico.
Descripción:	En equipos biométricos
Características del lugar donde se resguardan los soportes:	Los soportes electrónicos se encuentran en dos equipos biométricos ubicados como se muestra en la Figura 2. Los equipos se encuentran asegurados con una llave especial y en el acceso al edificio se encuentra personal de vigilancia.

3. ANÁLISIS DE RIESGOS

Información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

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

5. PLAN DE TRABAJO

Información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

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



Defensoría de los
Derechos Universitarios
Igualdad y Atención de
la Violencia de Género

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Departamento de Sistemas	
Identificador único	<u>SDUCA</u>
Nombre del sistema	<u>Sistema de Control de Acceso</u>
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos	El sistema no genera soportes físicos.
Transferencias mediante el traslado de soportes electrónicos	No se realiza transferencia de soportes electrónicos de datos personales.
Transferencias mediante el traslado sobre redes electrónicas	No hay traslado de los datos biométricos de los empleados a través de la red electrónica, estos permanecen almacenados solamente en los equipos de control de acceso.

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

No aplica ya que se trata de soportes electrónicos.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El sistema cuenta con registros electrónicos de eventos de operación que se guardan en la base de datos por un periodo indefinido, almacenando el nombre de usuario, fecha y hora de ingreso o salida.

Para asegurar la integridad de la bitácora, solamente el administrador del sistema tiene acceso a los registros mediante el dispositivo biométrico.

La bitácora es revisada aleatoriamente por el administrador del sistema. No se cuenta con herramienta para su análisis automático por lo que se realiza de manera manual.

IV. REGISTRO DE INCIDENTES

En el procedimiento de atención a incidentes se contemplará:

- a) Nombre de la persona que gestionó el incidente
- b) Fecha, hora y lugar del incidente
- c) Afectación y alcance del incidente
- d) Metodología aplicada
- e) Soportes electrónicos afectados

Para el caso de cualquier incidente, el responsable del sistema dará vista al titular del área universitaria para su conocimiento, así como al Responsable de Seguridad de Datos Personales, para que en el ámbito de sus atribuciones determinen lo conducente.

En el caso de robo o extravío de datos personales, se alertará a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior:

El edificio donde se encuentran las instalaciones cuenta con vigilancia las 24 horas, el control de acceso a la dependencia es mediante equipo biométrico.

Al tratarse de un área que brinda asistencia a la comunidad universitaria en general, las personas que acceden a las instalaciones:

- a) No tienen que identificarse



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

- b) La autenticación mediante huella es necesaria para el personal de la Defensoría
- c) En caso de personas ajenas a la Defensoría, se les da acceso a personas que solicitan atención para casos que este órgano universitario está facultado para atender.

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

Los soportes electrónicos se encuentran en los equipos biométricos.

Para las personas que acceden a dichos espacios interiores:

- c) Sólo tiene acceso el personal de la Defensoría
- d) El acceso se autoriza a solicitud del personal con acceso autorizado a los expedientes.

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

Cualquier rectificación de datos personales se deberá ceñir a los procedimientos institucionales consignados en la normatividad universitaria aplicable en la materia de protección de datos personales (Derechos ARCO).

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

- 1. El modelo de control de acceso para los equipos está basado en roles.
- 2. Perfiles de usuario y contraseñas manejados por el software del equipo biométrico:
 - a) Tiene un manejo riguroso de perfiles de usuario y contraseña.
 - b) La contraseña usada para los roles de administración son los datos biométricos.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

3. Administración de perfiles de usuario y contraseñas:

- a) El jefe del Departamento de Sistema da de alta los nuevos usuarios.
- b) Esto se hace previa autorización de la titular.
- c) En la base de datos se registra la fecha en que realizó el alta.

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

- a) Se utiliza contraseña de administrador para la conexión remota a los equipos, así como las direcciones IP de los mismos.
- b) El administrador requiere acceso remoto al servidor de aplicaciones ya que es necesario para la solución de incidentes o consulta de información requerida en horarios fuera de oficina, debido a la naturaleza de los casos que se atiende.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

- 1. Los respaldos se realizan de acuerdo con la política del Centro de Datos de la UNAM
 - a) Completo 1
 - b) Periodicidad con que los realiza: mensual
- 2. Se utiliza el equipo de cómputo del administrador.
- 3. Esta se ubica en las oficinas centrales.
- 4. Los responsables de la realización de los respaldos, es el personal del Centro de Datos de la UNAM.

IX. PLAN DE CONTINGENCIA

La información contenida en los dispositivos biométricos puede ser recuperada y restaurada para su operación mediante la exportación de los mismos.

Se cuenta con un sitio alternativo en el antiguo edificio de posgrado con capacidad para hospedar parte del personal de la oficina central, restaurando la operación en un tiempo razonable.

El plan de contingencia se encuentra en desarrollo.



Defensoría de los
Derechos Universitarios
Igualdad y Atención de
la Violencia de Género

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

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

Departamento de Sistemas		
Identificador único	SDUCA	
Nombre del sistema	Sistema de Control de Acceso	
Recurso	Descripción	Control
Software de administración	Revisiones aleatorias a los logs de operación de los biométricos.	El jefe del Departamento de Sistema analiza los registros de actividad inusual

7.2 Procedimiento para la revisión de las medidas de seguridad

Departamento de Sistemas		
Identificador único	SDUCA	
Nombre del sistema	Sistema de Control de Acceso	
Medida de seguridad	Procedimiento	Responsable
Pruebas de extracción	Se realizarán pruebas de extracción de registros.	a) Ing. Héctor Javier Correa Peragallo b) 5 días

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

Departamento de Sistemas



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Identificador único	SDUCA	
Nombre del sistema	Sistema de Control de Acceso	
Medida de seguridad	Resultado de evaluación	Responsable
Actualización de firmware	El dispositivo ya no cuenta con soporte por parte del fabricante por lo que no hay actualizaciones de seguridad	a) Ing. Héctor Javier Correa Peragallo b) Noviembre de 2022

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

Departamento de Sistemas		
Identificador único	SDUCA	
Nombre del sistema	Sistema de Control de Acceso	
Medida de seguridad	Acciones	Responsable
Actualización de contraseñas	Se actualizaron las contraseñas de acceso a la aplicación.	c) Ing. Héctor Javier Correa Peragallo d) Diciembre de 2022.



8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Departamento de Sistemas			
Identificador único		<u>SDUCA</u>	
Nombre del sistema		<u>Sistema de Control de Acceso</u>	
Actividad	Descripción	Duración	Cobertura
Curso Medidas de seguridad técnicas para la protección de datos personales	Curso en línea impartido por la DGTIC	Del 8 de febrero al 14 de marzo de 2021, con duración equivalente a 25 horas.	Personal del Departamento de Sistemas.
Programa de capacitación sobre protección de datos personales	Impartido en conjunto por la DGTIC y la Unidad de Transparencia	Del 22 al 25 de marzo, de 12 a 14:30	Personal involucrado en el desarrollo del documento de seguridad

8.2 PROGRAMA DE DIFUSIÓN DE LA PROTECCIÓN A LOS DATOS PERSONALES

Departamento de Sistemas			
Identificador único		<u>SDUCA</u>	
Nombre del sistema		<u>Sistema de Control de Acceso</u>	
Actividad	Descripción	Duración	Cobertura
Difusión sobre seguridad informática	Sitio web con información sobre vulnerabilidades, riesgos, amenazas y buenas prácticas, el cual se difundió entre el personal	Sitio activo para difusión entre el personal de nuevo ingreso o que tiene acceso al sistema de gestión	Personal involucrado en el tratamiento de datos personales

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Departamento de Sistemas	
Identificador único	<u>SDUCA</u>



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Nombre del sistema		<u>Sistema de Control de Acceso</u>	
Actividad	Descripción	Duración	Cobertura
Contrato de mantenimiento preventivo	Se evaluará la adquisición de nuevos equipos	2 meses	Personal de la Defensoría

9.2 Actualización y mantenimiento de equipo de cómputo

Departamento de Sistemas			
Identificador único		<u>SDUCA</u>	
Nombre del sistema		<u>Sistema de Control de Acceso</u>	
Actividad	Descripción	Duración	Cobertura
Revisión de espacio de almacenamiento de equipos	El administrador realiza la revisión periódica del espacio de almacenamiento de los equipos para el registro de usuarios y eventos	1 hora	Personal de la Defensoría
Actualización de firmware	Se realizó el mantenimiento preventivo de los equipos de control de acceso, con lo que se actualizó el firmware con las mejoras realizadas por el fabricante	Tres horas, con inicio y fin el 16 de mayo del 2021	La actualización en el firmware permite corregir posibles fallos o vulnerabilidades

9.3 Procesos para la conservación, preservación y respaldos de información

Departamento de sistemas	
Identificador único	<u>SDUCA</u>



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Nombre del sistema	<u>Sistema de Control de Acceso</u>	
Proceso	Descripción	Responsable
Respaldo en línea	Se realiza mensualmente la descarga y respaldo de los eventos de los dispositivos biométricos	1) Ing. Héctor Javier Correa Peragallo 2) 1 día

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

Departamento de sistemas		
Identificador único	<u>SDUCA</u>	
Nombre del sistema	<u>Sistema de Control de Acceso</u>	
Proceso	Descripción	Responsable
Borrado de memoria	Al cambiar el equipo biométrico, la memoria con los registros deberá se extraída y destruida.	1) Ing. Héctor Javier Correa Peragallo 2) 1 días

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

El procedimiento para la cancelación del sistema se encuentra en desarrollo y se tiene contemplado:



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

- Elaboración de solicitud de cancelación justificada
- Notificación a los usuarios de los dispositivos biométricos
- Suspensión y remoción de los dispositivos
- Borrado seguro de los registros



C. Sistema de Video Vigilancia

I. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Identificador único:	<u>SDUVV</u>
Nombre del sistema:	<u>Sistema de Video Vigilancia</u>
Datos personales contenidos en el sistema:	Datos de identificación: • Videos
Responsable	
Nombre:	Julia Elena Santiago Velasco
Cargo:	Jefa de la Unidad Administrativa
Funciones:	Administrar y dar seguimiento al sistema para el adecuado desarrollo y funcionamiento de los recursos financieros, humanos, materiales y servicios con que cuenta la dependencia.
Obligaciones:	Guardar la confidencialidad de la información relativa los videos de vigilancia, haciendo uso exclusivo para los fines que hayan sido recabados.
Encargado	
Nombre	Héctor Javier Correa Peragallo
Cargo:	Jefe de Departamento
Funciones:	Monitorear el funcionamiento y manejo del sistema. Adoptar las medidas necesarias para asegurar el correcto funcionamiento y disponibilidad del sistema.
Obligaciones:	Guardar la confidencialidad de la información relativa los videos de vigilancia, haciendo uso exclusivo para los fines que hayan sido recabados.

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

Departamento de sistemas	
Identificado único:	<u>SDUVV</u>
Nombre del sistema:	Sistema de Video Vigilancia



Tipo de soporte:	El sistema se encuentra en soporte electrónico.
Descripción:	Los soportes se encuentran en un DVR
Características del lugar donde se resguardan los soportes:	El DVR se encuentra en el rack de telecomunicaciones al cual se accede sólo con llave, este está ubicado en la oficina del área de sistemas a la cual se accede con llave.

Información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

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



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

4. ANÁLISIS DE BRECHA

Información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

5. PLAN DE TRABAJO

Información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

--



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Departamento de sistemas	
Identificador único	<u>SDUVV</u>
Nombre del sistema	Sistema de Video Vigilancia
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	El sistema no genera soportes físicos
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de los videos almacenados en los



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

	equipos de video grabación.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias a través de redes de los videos almacenados en los equipos de video grabación.

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

No aplica ya que se trata de soportes electrónicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El sistema cuenta con registros electrónicos de eventos de operación que se guardan en la base de datos por un periodo definido por la capacidad de disco duro y las grabaciones, almacenando fecha, hora, tipo de evento, canal, usuario e IP.

Para asegurar la integridad de la bitácora, solamente el administrador del sistema tiene acceso a los registros.

La bitácora es revisada aleatoriamente por el administrador del sistema. No se cuenta con herramienta para su análisis automático por lo que se realiza de manera manual.

IV. REGISTRO DE INCIDENTES

En el procedimiento de atención a incidentes se contemplará:

- a) Nombre de la persona que gestionó el incidente
- b) Fecha, hora y lugar del incidente
- c) Afectación y alcance del incidente
- d) Metodología aplicada
- e) Soportes electrónicos afectados

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior:



El edificio donde se encuentran las instalaciones cuenta con vigilancia las 24 horas, el control de acceso a la dependencia es mediante equipo biométrico, se cuenta con equipo de video vigilancia que resguarda los videos en el disco duro de un DVR.

Al tratarse de un área que brinda asistencia a la comunidad universitaria en general, las personas que acceden a las instalaciones:

- a) No tienen que identificarse
- b) La autenticación mediante huella es necesaria para el personal de la Defensoría
- c) En caso de personas ajenas a la Defensoría, se les da acceso a personas que solicitan atención para casos que este órgano universitario está facultado para atender.

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

Los soportes electrónicos se encuentran en los equipos de video grabación alojados en el rack de telecomunicaciones.

Para las personas que acceden a dichos espacios interiores:

- a) Sólo tiene acceso el personal de la Defensoría
- b) El acceso se autoriza a solicitud de algún registro en video.

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

Cualquier rectificación de datos personales se deberá ceñir a los procedimientos institucionales consignados en la normatividad universitaria aplicable en la materia de protección de datos personales (Derechos ARCO).

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. El modelo de control de acceso para los equipos del personal está basado en roles.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

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

- a) Tiene un manejo riguroso de perfiles de usuario y contraseña.
- b) La contraseña de los usuarios se guarda de manera cifrada en la base de datos.

3. Administración de perfiles de usuario y contraseñas:

- a) El jefe del Departamento de Sistema da de alta los nuevos perfiles.
- b) Esto se hace previa autorización de la titular.

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

- a) Los equipos de video grabación cuentan con dirección IP, por lo que pueden ser accedidos de manera remota.
- b) El acceso remoto no autorizado puede ser revisado en los logs del sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Los respaldos se realizan de manera parcial
 - a) Bajo demanda.
2. Se utiliza un NAS para el almacenamiento de los respaldos.
3. Este se ubica, en el rack de telecomunicaciones de las oficinas centrales.
4. Los responsables de la realización de los respaldos, es el personal del departamento de sistemas de la Defensoría.

IX. PLAN DE CONTINGENCIA

La información contenida en los equipos de grabación puede ser recuperada para su operación mediante la exportación de los mismos.

Se cuenta con un sitio alternativo en el antiguo edificio de posgrado con capacidad para hospedar parte del personal de la oficina central, restaurando la operación en un tiempo razonable.

El plan de contingencia se encuentra en desarrollo.



Defensoría de los
Derechos Universitarios
Igualdad y Atención de
la Violencia de Género

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

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

Departamento de Sistemas		
Identificador único	<u>SDUVV</u>	
Nombre del sistema	<u>Sistema de Video Vigilancia</u>	
Recurso	Descripción	Control
Software de administración	Revisiones aleatorias a los logs de operación de los equipos de video grabación	El jefe del Departamento de Sistema analiza los registros de actividad inusual

7.2 Procedimiento para la revisión de las medidas de seguridad

Departamento de Sistemas		
Identificador único	<u>SDUVV</u>	
Nombre del sistema	<u>Sistema de Video Vigilancia</u>	
Medida de seguridad	Procedimiento	Responsable
Pruebas de extracción	Se realizarán pruebas de extracción de registros.	Ing. Héctor Javier Correa Peragallo) 3 días

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

Departamento de Sistemas



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Identificador único	<u>SDUVV</u>	
Nombre del sistema	<u>Sistema de Video Vigilancia</u>	
Medida de seguridad	Resultado de evaluación	Responsable
Actualización de firmware	El dispositivo ya no cuenta con soporte por parte del fabricante por lo que no hay actualizaciones de seguridad	a) Ing. Héctor Javier Correa Peragallo b) Noviembre de 2022

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

Departamento de Sistemas		
Identificador único	<u>SDUVV</u>	
Nombre del sistema	<u>Sistema de Video Vigilancia</u>	
Medida de seguridad	Acciones	Responsable
Actualización de contraseñas	Se actualizaron las contraseñas de acceso a la aplicación.	a) Ing. Héctor Javier Correa Peragallo b) Noviembre de 2022.



8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Departamento de Sistemas			
Identificador único		<u>SDUVV</u>	
Nombre del sistema		<u>Sistema de Video Vigilancia</u>	
Actividad	Descripción	Duración	Cobertura
Curso Medidas de seguridad técnicas para la protección de datos personales	Curso en línea impartido por la DGTIC	Del 8 de febrero al 14 de marzo de 2021, con duración equivalente a 25 horas.	Personal del Departamento de Sistemas.
Programa de capacitación sobre protección de datos personales	Impartido en conjunto por la DGTIC y la Unidad de Transparencia	Del 22 al 25 de marzo, de 12 a 14:30	Personal involucrado en el desarrollo del documento de seguridad

8.2 Programa de difusión de la protección a los datos personales

Departamento de Sistemas			
Identificador único		<u>SDUVV</u>	
Nombre del sistema		<u>Sistema de Video Vigilancia</u>	
Actividad	Descripción	Duración	Cobertura
Difusión sobre seguridad informática	Sitio web con información sobre vulnerabilidades, riesgos, amenazas y buenas prácticas, el cual se difundió entre el personal	Sitio activo para difusión entre el personal de nuevo ingreso o que tiene acceso al sistema de gestión	Personal involucrado en el tratamiento de datos personales

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Departamento de Sistemas	
Identificador único	<u>SDUVV</u>



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Nombre del sistema		Sistema de Video Vigilancia	
Actividad	Descripción	Duración	Cobertura
Contrato de mantenimiento preventivo	Se realizó la contratación del mantenimiento preventivo del sistema	1 día	Personal y personas atendidas de manera presencial

9.2 Actualización y mantenimiento de equipo de cómputo

Departamento de Sistemas			
Identificador único		<u>SDUVV</u>	
Nombre del sistema		<u>Sistema de Video Vigilancia</u>	
Actividad	Descripción	Duración	Cobertura
Mantenimiento preventivo	Se realizó el mantenimiento preventivo anual a los equipos DVR	Cuatro horas	Se busca mejorar las condiciones de operación de los equipos, para prevenir fallas en los mismos

9.3 Procesos para la conservación, preservación y respaldos de información

Departamento de sistemas		
Identificador único		<u>SDUVV</u>
Nombre del sistema		<u>Sistema de Video Vigilancia</u>
Proceso	Descripción	Responsable
Respaldo	Se realiza a solicitud de la titular, defensores adjuntos o Jefa de la Unidad Administrativa.	1) Ing. Héctor Javier Correa Peragallo 2) 1 día



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

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

Departamento de sistemas		
Identificador único	<u>SDUVV</u>	
Nombre del sistema	<u>Sistema de Video Vigilancia</u>	
Proceso	Descripción	Responsable
Borrado de disco duro	Al cambiar el disco duro se realiza el borrado permanente a bajo nivel y se llena el formato de borrado seguro correspondiente.	1) Ing. Héctor Javier Correa Peragallo 2) 1 días

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

El procedimiento para la cancelación del sistema se encuentra en desarrollo y se tiene contemplado:

- Elaboración de solicitud de cancelación justificada
- Notificación a los usuarios autorizados para solicitar videos de respaldo
- Suspensión y remoción de los dispositivos
- Borrado seguro de los registros



Defensoría de los
Derechos Universitarios
Igualdad y Atención de
la Violencia de Género

D. Sistema Integral de Personal

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Identificador único:	<u>SIP</u>
Nombre del sistema:	<u>Sistema Integral de Personal</u>
Datos personales contenidos en el sistema:	Datos de identificación: • Nombre • Domicilio • Teléfono particular • Teléfono celular • Correo electrónico • Fecha de nacimiento • CURP
Responsable	
Nombre:	Dirección General de Personal
Cargo:	Dirección de Sistemas y Nómina
Funciones:	Responder a los requerimientos de información de las entidades y dependencias universitarias, impulsar los proyectos de mejora y actualización y proporcionar soporte técnico.
Obligaciones:	Asegurar la confidencialidad, integridad y disponibilidad de los datos personales almacenados en el sistema.
Encargada	
Nombre:	Julia Elena Santiago Velasco
Cargo:	Jefa de la Unidad Administrativa
Funciones:	Registro de altas y bajas del personal, información para pago de marcha, solicitud de credencial, cambio de domicilio y promociones.
Obligaciones:	Mantener las medidas de seguridad que permitan proteger los datos personales contra pérdida, alteración, acceso o tratamiento no autorizado.
Usuario	
Nombre:	Guadalupe Barrera Nájera
Cargo:	Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género



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

3. ANÁLISIS DE RIESGOS

Información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Category	Value
Category 1	100
Category 2	20
Category 3	10



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

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

5. PLAN DE TRABAJO

Información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

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



Defensoría de los
Derechos Universitarios
Igualdad y Atención de
la Violencia de Género

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Unidad Administrativa	
Identificador único	<u>SIP</u>
Nombre del sistema	<u>Sistema Integral de Personal</u>
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos	La documentación del personal requerida por la Dirección General de Asuntos Jurídicos se remite mediante el gestor de la Defensoría directamente en las oficinas de la dirección en sobre cerrado, con oficio y solicitando acuse de recibo.
Transferencias mediante el traslado de soportes electrónicos	No se realizan transferencias de datos personales en soporte electrónico.
Transferencias mediante el traslado sobre redes electrónicas	No se realizan transferencias de datos personales mediante redes electrónicas.

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

Los expedientes del personal se encuentran en gabinetes dentro de un área resguardada bajo llave.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El sistema es administrado por la Dirección General de Personal de la UNAM, por lo que las bitácoras de acceso y operación no están disponibles para los usuarios de la aplicación.

En el caso de los accesos físicos a las áreas que cuentan con los expedientes del personal, estos pueden ser consultados a través de las video grabaciones mediante solicitud de la Jefa de la Unidad Administrativa.

IV. REGISTRO DE INCIDENTES

En el procedimiento de atención a incidentes se contemplará:

- a) Nombre de la persona que gestionó el incidente
- b) Fecha, hora y lugar del incidente
- c) Afectación y alcance del incidente
- d) Metodología aplicada
- e) Soportes físicos afectados

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior:

El edificio donde se encuentran las instalaciones cuenta con vigilancia las 24 horas, el control de acceso a la dependencia es mediante equipo biométrico, se cuenta con equipo de video vigilancia que resguarda los videos en el disco duro de un DVR.

Al tratarse de un área que brinda asistencia a la comunidad universitaria en general, las personas que acceden a las instalaciones:

- a) No tienen que identificarse
- b) La autenticación mediante huella es necesaria para el personal de la Defensoría
- c) En caso de personas ajenas a la Defensoría, se les da acceso a personas que solicitan atención para casos que este órgano universitario está facultado para atender.

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



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Para los soportes físicos que se encuentran en gavetas dentro de la Unidad Administrativa, se cuenta con vigilancia 24 horas en el edificio, el control de acceso a la dependencia es mediante equipo biométrico, se cuenta con equipo de video vigilancia que resguarda los videos en el disco duro de un DVR y el acceso a la oficina donde se encuentra el archivo es mediante llave.

Para las personas que acceden a dichos espacios interiores:

- a) Sólo tiene acceso el personal de la Defensoría
- b) El acceso se autoriza a solicitud del personal con acceso autorizado a los expedientes.

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

Cualquier rectificación de datos personales se deberá ceñir a los procedimientos institucionales consignados en la normatividad universitaria aplicable en la materia de protección de datos personales (Derechos ARCO).

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. El modelo de control de acceso para el aplicativo del sistema está basado en roles.
2. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
 - a) Tiene un manejo riguroso de perfiles de usuario y contraseña.
 - b) La contraseña de los usuarios se guarda de manera cifrada en la base de datos.
3. Administración de perfiles de usuario y contraseñas:
 - a) Para dar alta los nuevos perfiles se solicita por oficio a la Dirección General de Personal de la UNAM.
 - b) Esto se hace previa autorización de la jefa de la Unidad Administrativa.
4. Acceso remoto al sistema de tratamiento de datos personales:



- a) Para el acceso remoto al aplicativo, es necesario contar con una dirección de una red privada de datos proporcionada por la Dirección General de Personal de la UNAM.
- b) El acceso remoto no autorizado al servidor de aplicaciones y base de datos está restringido por un certificado con llave primaria y contraseña segura.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Los respaldos se realizan de manera parcial bajo demanda.
2. Se solicita a la Dirección General de Personal de la UNAM.
3. El respaldo es entregado en un medio de almacenamiento óptico.
4. Los responsables de la realización de los respaldos, es el personal de la Dirección General de Personal de la UNAM.

IX. PLAN DE CONTINGENCIA

La información contenida en los expedientes físicos, puede ser consultada en el sistema para los propósitos que sean útiles al área administrativa.

Se cuenta con un sitio alterno tibio en el antiguo edificio de posgrado con capacidad para hospedar parte del personal de la oficina central, restaurando la operación en un tiempo razonable.

El plan de contingencia se encuentra en desarrollo.

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

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

Unidad Administrativa		
Identificador único	<u>SIP</u>	
Nombre del sistema	<u>Sistema Integral de Personal</u>	
Recurso	Descripción	Control
Cámara de video vigilancia	Revisiones aleatorias al equipo biométrico de control	La verificación se realiza por parte del personal con acceso



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

	de acceso ubicado en el acceso a las instalaciones	al sistema de monitoreo del equipo de video vigilancia
--	---	---

7.2 Procedimiento para la revisión de las medidas de seguridad

Departamento de Sistemas		
Identificador único	<u>SIP</u>	
Nombre del sistema	<u>Sistema Integral de Personal</u>	
Medida de seguridad	Procedimiento	Responsable
Evaluación de medidas actuales	Se evaluaron las medidas de seguridad con los que cuentan los expedientes físicos del personal de la Defensoría.	a) Personal de la Unidad Administrativa. b) 3 días

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

Departamento de Sistemas		
Identificador único	<u>SIP</u>	
Nombre del sistema	<u>Sistema Integral de Personal</u>	
Medida de seguridad	Resultado de evaluación	Responsable



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Análisis de la evaluación	Identificar vulnerabilidades de seguridad	) Personal de la Unidad Administrativa.) Noviembre de 2022
---------------------------	---	--

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

Departamento de Sistemas		
Identificador único	<u>SIP</u>	
Nombre del sistema	<u>Sistema Integral de Personal</u>	
Medida de seguridad	Acciones	Responsable
Video vigilancia	Se instaló una cámara para monitorear el acceso a las oficinas de la Unidad Administrativa	a) Ing. Héctor Javier Correa Peragallo b) febrero de 2023.
Solicitud al personal	Concientizar al personal de la Unidad Administrativa para mantener resguardado bajo llave de manera permanente los archiveros donde se encuentran los expedientes físicos del personal.	Jefa de la Unidad Administrativa, de manera recurrente.



8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Unidad Administrativa			
Identificador único		<u>SIP</u>	
Nombre del sistema		<u>Sistema Integral de Personal</u>	
Actividad	Descripción	Duración	Cobertura
Curso Medidas de seguridad técnicas para la protección de datos personales	Curso en línea impartido por la DGTIC	Del 8 de febrero al 14 de marzo de 2021, con duración equivalente a 25 horas.	Personal del Departamento de Sistemas.
Programa de capacitación sobre protección de datos personales	Impartido en conjunto por la DGTIC y la Unidad de Transparencia	Del 22 al 25 de marzo, de 12 a 14:30	Personal involucrado en el desarrollo del documento de seguridad

8.2 Programa de difusión de la protección a los datos personales

Unidad Administrativa			
Identificador único		<u>SIP</u>	
Nombre del sistema		<u>Sistema Integral de Personal</u>	
Actividad	Descripción	Duración	Cobertura
Difusión sobre seguridad informática	Sitio web con información sobre vulnerabilidades, riesgos, amenazas y buenas prácticas, el cual se difundió entre el personal	Sitio activo para difusión entre el personal de nuevo ingreso o que tiene acceso al sistema de gestión	Personal involucrado en el tratamiento de datos personales

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Unidad Administrativa	
Identificador único	<u>SIP</u>



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Nombre del sistema		<u>Sistema Integral de Personal</u>	
Actividad	Descripción	Duración	Cobertura
Instalación de cámara de seguridad	Se realizó la instalación de un equipo de video vigilancia para monitorear las áreas con los expedientes	1 día	Personal de la Defensoría

9.2 Actualización y mantenimiento de equipo de cómputo

Unidad Administrativa			
Identificador único		<u>SIP</u>	
Nombre del sistema		<u>Sistema Integral de Personal</u>	
Actividad	Descripción	Duración	Cobertura
Protección perimetral	Se instaló antivirus con protección de intrusiones	1 día	Personal de la Defensoría

9.3 Procesos para la conservación, preservación y respaldos de información

No aplica ya que se trata de soportes físicos, siendo la Dirección General de Personal de la UNAM la entidad que administra el sistema, bases de datos y servidor que los aloja, para el caso de la Defensoría, solo se cuenta con acceso a la aplicación para alimentar y actualizar información.

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

No aplica ya que se trata de soportes físicos.

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

El procedimiento para la cancelación del sistema se encuentra en desarrollo y se tiene contemplado:

- Elaboración de solicitud de cancelación justificada



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

- Notificación a los usuarios con acceso al sistema
- Desinstalación de los accesos a las aplicaciones



E. Sistema Institucional de Compras

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Identificador único:	<u>SIC</u>
Nombre del sistema:	<u>Sistema Institucional de Compras</u>
Datos personales contenidos en el sistema:	Datos de identificación: • Nombre • Teléfono • Correo electrónico • RFC
Responsable	
Nombre:	Dirección General de Proveeduría
Cargo:	Dirección de Normatividad y Desarrollo Tecnológico
Funciones:	Responder a los requerimientos de información de las entidades y dependencias universitarias, impulsar los proyectos de mejora y actualización y proporcionar soporte técnico.
Obligaciones:	Asegurar la confidencialidad, integridad y disponibilidad de los datos personales almacenados en el sistema.
Encargada	
Nombre:	Julia Elena Santiago Velasco
Cargo:	Jefa de la Unidad Administrativa
Funciones:	Asignación de claves presupuestales y firma para trámite de pago a proveedores.
Obligaciones:	Mantener las medidas de seguridad que permitan proteger los datos personales contra pérdida, alteración, acceso o tratamiento no autorizado.
Usuarios	
Nombre 1:	Guadalupe Barrera Nájera
Cargo:	Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género
Funciones:	Autorización de trámites y solicitudes.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Obligaciones:	Mantener las medidas de seguridad que permitan proteger los datos personales contra pérdida, alteración, acceso o tratamiento no autorizado.
Nombre 2:	Ilse Paulina Huerta Ramírez
Cargo:	Jefa de Unidad
Funciones:	Registro de la solicitud de pago a proveedores de algún producto o servicio, se registra el RFC, Nombre o Razón Social, teléfono y correo electrónico, así como los datos y documentos necesarios para proceder al pago (transferencia).
Obligaciones:	Mantener las medidas de seguridad que permitan proteger los datos personales contra pérdida, alteración, acceso o tratamiento no autorizado.

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

Unidad Administrativa	
Identificado único:	<u>SIC</u>
Nombre del sistema:	<u>Sistema Institucional de Compras</u>
Tipo de soporte:	El sistema se encuentra en soporte electrónico y físico.
Descripción:	Los soportes físicos se encuentran en expedientes físicos y los soportes digitales en bases de datos dentro de servidores.
Características del lugar donde se resguardan los soportes:	Los soportes físicos están almacenados en un archivero con llave, dentro de la oficina de la Unidad Administrativa con llave de acceso, con una dimensión de 9.51 metros cuadrados. Los soportes digitales se encuentran en el Centro de Datos del Centro de Cómputo Pitágoras de la UNAM.

3. ANÁLISIS DE RIESGOS

Información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

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

5. PLAN DE TRABAJO

Información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

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



Defensoría de los
Derechos Universitarios
Igualdad y Atención de
la Violencia de Género

6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Unidad Administrativa	
Identificador único	<u>SIC</u>
Nombre del sistema	<u>Sistema Institucional de Compras</u>
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos	No se realiza transferencia de los datos personales de los proveedores.
Transferencias mediante el traslado de soportes electrónicos	No se realiza transferencia de los datos personales de los proveedores.
Transferencias mediante el traslado sobre redes electrónicas	No se realiza transferencia de los datos personales de los proveedores.

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

1. Medidas de seguridad implementadas para el resguardo de los soportes físicos del sistema:

Los expedientes con la información de los proveedores se encuentran en gabinetes dentro de un área resguardada bajo llave.

2. Listado de personas que tienen acceso a los soportes físicos del sistema:



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Identificador único:	<u>SIC</u>
Nombre del sistema:	<u>Sistema Institucional de Compras</u>
Responsable	
Nombre:	Julia Elena Santiago Velasco
Cargo:	Jefa de la Unidad Administrativa
Funciones:	Administrar los recursos financieros, humanos, materiales y servicios con que cuenta la dependencia, para su desarrollo y funcionamiento, dando apoyo a las áreas de la Defensoría y alcanzar las metas encomendadas.
Obligaciones:	Supervisar los procesos relacionados con la administración en el cambio de la situación laboral del personal administrativo de base, confianza y funcionario. Rendir informes periódicos del estado que guarda la Defensoría de los Derechos Universitarios y de los asuntos encomendados por el Titular. Guardar la confidencialidad de la información relativa los datos biométricos, haciendo uso exclusivo para los fines que hayan sido recabados.
Personal autorizado	
Nombre	Guadalupe Barrera Nájera
Cargo:	Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género
Funciones:	Coordina el trámite de los asuntos por violencia de género y derechos universitarios, y suscribe los oficios, acuerdos y recomendaciones para su determinación. Coordinar la administración y distribución correcta de los recursos humanos, materiales, tecnológicos y financieros, asignados al área para el cumplimiento de las actividades encomendadas. Mantener comunicación con las distintas autoridades universitarias internas y externas para tratar asuntos materia de su competencia. Supervisar y vigilar que los sistemas de control se lleven a cabo, a efecto de conocer permanentemente el avance de los asuntos competencia de la Dirección. Coordinar, promover y vigilar el desarrollo de los programas sustantivos y de gestión interna, a efecto de propiciar los conceptos de mejora continua y calidad total, en cumplimiento



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

	a los lineamientos, políticas, contratos colectivos de trabajo y normatividad vigentes en la UNAM, en materia de administración de personal. Establecer normas, políticas, procedimientos y programas internos que promuevan y controlen las actividades que se desarrollan en la Dependencia.
Nombre	Ilse Paulina Huerta Ramírez
Cargo:	Jefa de Unidad
Funciones:	Registro de la solicitud de pago a proveedores de algún producto o servicio, se registra el RFC, Nombre o Razón Social, teléfono y correo electrónico, así como los datos y documentos necesarios para proceder al pago (transferencia).
Obligaciones:	Mantener las medidas de seguridad que permitan proteger los datos personales contra pérdida, alteración, acceso o tratamiento no autorizado.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA:

El sistema es administrado por la Dirección General de Proveeduría de la UNAM, por lo que las bitácoras de acceso y operación no están disponibles para los usuarios de la aplicación.

En el caso de los accesos físicos a las áreas que cuentan con los expedientes del personal, estos pueden ser consultados a través de las video grabaciones mediante solicitud de la Jefa de la Unidad Administrativa.

IV. REGISTRO DE INCIDENTES

En el procedimiento de atención a incidentes se contemplará:

- Nombre de la persona que gestionó el incidente
- Fecha, hora y lugar del incidente
- Afectación y alcance del incidente
- Metodología aplicada
- Soportes físicos afectados

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior:



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

El edificio donde se encuentran las instalaciones cuenta con vigilancia las 24 horas, el control de acceso a la dependencia es mediante equipo biométrico, se cuenta con equipo de video vigilancia que resguarda los videos en el disco duro de un DVR.

Al tratarse de un área que brinda asistencia a la comunidad universitaria en general, las personas que acceden a las instalaciones:

- a) No tienen que identificarse
- b) La autenticación mediante huella es necesaria para el personal de la Defensoría
- c) En caso de personas ajenas a la Defensoría, se les da acceso a personas que solicitan atención para casos que este órgano universitario está facultado para atender.

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

Los soportes electrónicos se encuentran en el Centro de Datos de la Dirección General de Proveeduría de la UNAM, por lo que las medidas de seguridad perimetral interior deberán obrar en el documento de dicha dependencia.

Para los soportes físicos que se encuentran en la Unidad Administrativa, se cuenta con vigilancia 24 horas en el edificio, el control de acceso a la dependencia es mediante equipo biométrico, se cuenta con equipo de video vigilancia que resguarda los videos en el disco duro de un DVR y el acceso a la oficina donde se encuentra el archivo es mediante llave.

Para las personas que acceden a dichos espacios interiores:

- a) Sólo tiene acceso el personal de la Defensoría
- b) El acceso se autoriza a solicitud del personal con acceso autorizado a los expedientes.

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

Cualquier rectificación de datos personales se deberá ceñir a los procedimientos institucionales consignados en la normatividad universitaria aplicable en la materia de protección de datos personales (Derechos ARCO).



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. El modelo de control de acceso para los equipos del personal está basado en roles.
2. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
 - a) Tiene un manejo riguroso de perfiles de usuario y contraseña.
 - b) La contraseña de los usuarios se guarda de manera cifrada en la base de datos.
3. Administración de perfiles de usuario y contraseñas:
 - a) La Dirección General de Proveeduría es la encargada de la asignación de perfiles y contraseñas.
 - b) Esto se hace previa autorización de la titular.
4. Acceso remoto al sistema de tratamiento de datos personales:
 - a) Los usuarios del aplicativo web tienen acceso remoto al sistema mediante dirección IP autorizada.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Los respaldos se realizan de acuerdo con la política del Centro de Datos de la Dirección General de Proveeduría.

IX. PLAN DE CONTINGENCIA

La información contenida en los expedientes físicos, puede ser consultada en el sistema para los propósitos que sean útiles al área administrativa.

Se cuenta con un sitio alternativo en el antiguo edificio de posgrado con capacidad para hospedar parte del personal de la oficina central, restaurando la operación en un tiempo razonable.

El plan de contingencia se encuentra en desarrollo.



Defensoría de los
Derechos Universitarios
Igualdad y Atención de
la Violencia de Género

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

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

Departamento de Sistemas		
Identificador único	<u>SIC</u>	
Nombre del sistema	<u>Sistema Institucional de Compras</u>	
Recurso	Descripción	Control
Cámara de video vigilancia	Revisiones aleatorias al equipo biométrico de control de acceso ubicado en el acceso a las instalaciones	La verificación se realiza por parte del personal con acceso al sistema de monitoreo del equipo de video vigilancia

7.2 Procedimiento para la revisión de las medidas de seguridad

Departamento de Sistemas		
Identificador único	<u>SIC</u>	
Nombre del sistema	<u>Sistema Institucional de Compras</u>	
Medida de seguridad	Procedimiento	Responsable
Evaluación de medidas actuales	Se evaluaron las medidas de seguridad con los que cuentan los expedientes físicos del personal de la Defensoría.	a) Personal de la Unidad Administrativa. b) 3 días



Defensoría de los
Derechos Universitarios
Igualdad y Atención de
la Violencia de Género

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

Departamento de Sistemas		
Identificador único	<u>SIC</u>	
Nombre del sistema	<u>Sistema Institucional de Compras</u>	
Medida de seguridad	Resultado de evaluación	Responsable
Análisis de la evaluación	Identificar vulnerabilidades de seguridad	) Personal de la Unidad Administrativa.) Noviembre de 2022

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

Departamento de Sistemas		
Identificador único	<u>SIC</u>	
Nombre del sistema	<u>Sistema Institucional de Compras</u>	
Medida de seguridad	Acciones	Responsable
Video vigilancia	Se instaló una cámara para monitorear el acceso a las oficinas de la Unidad Administrativa	a) Ing. Héctor Javier Correa Peragallo b) febrero de 2023.



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Solicitud al personal	Concientizar al personal de la Unidad Administrativa para mantener resguardado bajo llave de manera permanente los archiveros donde se encuentran los expedientes de los proveedores.	Jefa de la Unidad Administrativa, de manera recurrente.
-----------------------	---	---

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Departamento de Sistemas			
Identificador único		<u>SIC</u>	
Nombre del sistema		<u>Sistema Institucional de Compras</u>	
Actividad	Descripción	Duración	Cobertura
Curso Medidas de seguridad técnicas para la protección de datos personales	Curso en línea impartido por la DGTIC	Del 8 de febrero al 14 de marzo de 2021, con duración equivalente a 25 horas.	Personal del Departamento de Sistemas.
Programa de capacitación sobre protección de datos personales	Impartido en conjunto por la DGTIC y la Unidad de Transparencia	Del 22 al 25 de marzo, de 12 a 14:30	Personal involucrado en el desarrollo del documento de seguridad

8.2 Programa de difusión de la protección a los datos personales

Departamento de Sistemas			
Identificador único		<u>SIC</u>	
Nombre del sistema		<u>Sistema Institucional de Compras</u>	
Actividad	Descripción	Duración	Cobertura



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

Difusión sobre seguridad informática	Sitio web con información sobre vulnerabilidades, riesgos, amenazas y buenas prácticas, el cual se difundió entre el personal	Sitio activo para difusión entre el personal de nuevo ingreso o que tiene acceso al sistema de gestión	Personal involucrado en el tratamiento de datos personales
--------------------------------------	---	--	--

9. MEJORA CONTINUA

9.1 Actualización y mantenimiento de sistemas de información

Unidad Administrativa			
Identificador único	<u>SIC</u>		
Nombre del sistema	<u>Sistema Institucional de Compras</u>		
Actividad	Descripción	Duración	Cobertura
Instalación de cámara de seguridad	Se realizó la instalación de un equipo de video vigilancia para monitorear las áreas con la información de los proveedores	1 día	Proveedores

9.2 Actualización y mantenimiento de equipo de cómputo

Departamento de Sistemas			
Identificador único	<u>SIC</u>		
Nombre del sistema	<u>Sistema Institucional de Compras</u>		
Actividad	Descripción	Duración	Cobertura
Protección perimetral	Se instaló antivirus con protección de intrusiones	1 día	Personal de la Defensoría

9.3 Procesos para la conservación, preservación y respaldos de información

No aplica ya que se trata de soportes físicos, siendo la Dirección General de Proveeduría de la UNAM la entidad que administra el sistema, bases de datos y



**Defensoría de los
Derechos Universitarios**
Igualdad y Atención de
la Violencia de Género

servidor que los aloja, para el caso de la Defensoría, solo se cuenta con acceso a la aplicación para alimentar y actualizar información.

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

No aplica ya que se trata de soportes físicos.

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

El procedimiento para la cancelación del sistema se encuentra en desarrollo y se tiene contemplado:

- Elaboración de solicitud de cancelación justificada
- Notificación a los usuarios con acceso al sistema
- Desinstalación de los accesos a las aplicaciones



Defensoría de los
Derechos Universitarios
Igualdad y Atención de
la Violencia de Género

Aprobación del documento de seguridad

Nombre y firma de quienes revisaron el presente documento

Responsable del desarrollo:

Ing. Héctor Javier Correa Peragallo
Jefe del Departamento de Sistemas
Tel: 555622 6106
hcorrea@defensoria.unam.mx

Revisó:

Mtro. César Flores Mancilla
Defensor Adjunto
Tel: 555622 6225
cflores@defensoria.unam.mx

Autorizó:

Dra. Guadalupe Barrena Nájera
Titular
Tel: 555622 6220
guadalupe@defensoria.unam.mx

Fecha de aprobación:

5 de agosto de 2022

Fecha de actualización:

01 de febrero de 2024



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/075/2024

Visto el expediente relativo a la clasificación de reserva parcial de la información para la elaboración de la versión pública que somete la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, en relación con su **Documento de Seguridad**, se procede a dictar la presente resolución con base en los siguientes:

ANTECEDENTES

- I. Con fecha 26 de enero de 2017 se publicó en el Diario Oficial de la Federación el Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.
- II. Mediante Acuerdo **ACT-PUB/19/12/2017.10**, de fecha 19 de diciembre de 2017, publicado en el Diario Oficial de la Federación con fecha 26 de enero de 2018, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- III. A través del Acuerdo **ACT-PUB/11/11/2020.05**, de fecha 11 de noviembre de 2020, publicado en el Diario Oficial de la Federación con fecha 25 de noviembre de 2020, dicho Órgano Garante aprobó la adición de un Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público, a fin de establecer las disposiciones generales que permiten desarrollar el procedimiento de diseño y aplicación del sistema y procedimiento para llevar a cabo la evaluación sobre el desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resultan aplicables en la materia.
- IV. Por Acuerdo **ACT-PUB/17/11/2021.05**, de fecha 17 de noviembre de 2021, publicado en el Diario Oficial de la Federación con fecha 26 de noviembre de 2021, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los “Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados”.
- V. Los numerales 247 y 248 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, así como las reglas Décima Tercera y Décima Cuarta del apartado “V. Reglas de Generales de Evaluación” del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establecen que la información y documentos que se pongan a disposición de los titulares de datos personales y del Instituto, deberán ser revisados por el responsable a fin de verificar que no contengan información confidencial o reservada y, de ser el caso, deberá publicarse la versión pública de dicha documentación.



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/075/2024

Por otra parte, en el apartado “VI. Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia”, Capítulo II. Criterios y formatos, **Vertiente 2: Deberes, Variable 2.1** Deber de seguridad, se establece que el responsable, por ningún motivo, debe publicar el documento de seguridad de manera íntegra, por lo que deberá poner a disposición la versión pública del mismo, en la cual se deberá proteger la información relativa al plan de trabajo, el análisis de riesgo y el análisis de brecha.

- VI.** En términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 34, fracción II del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, la clasificación de la información será procedente cuando, entre otros supuestos, se determiné mediante una resolución de autoridad competente.
- VII.** A través del oficio **DDUIAVG/T/0668/2024**, recibido con fecha 6 de febrero de 2024, dirigido a la Presidencia del Comité de Transparencia, la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género** comunicó lo siguiente:

“Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados¹; exige elaborar versión pública del documento de seguridad de esta área universitaria.

Una vez analizada la información que se solicitó en el primer punto del ‘Documento de seguridad’, se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.

En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los

¹ DOF: 26 de noviembre de 2021



COMITÉ DE TRANSPARENCIA DE LA
UNIVERSIDAD NACIONAL AUTÓNOMA DE
MÉXICO

RESOLUCIÓN: CTUNAM/075/2024

Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	Contenido y su afectación	Páginas
a) Análisis de riesgos	<i>El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.</i>	<i>22 a 23; 41; 52; 61; 71 a 72</i>
b) Análisis de brecha	<i>El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.</i>	<i>23 a 24; 42; 52; 62; 72</i>
c) Plan de Trabajo	<i>El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.</i>	<i>25 a 26; 42; 52 a 53; 62; 72</i>

Los fundamentos y motivos se exponen a continuación:

- Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los documentos consistentes en análisis de riesgo, el análisis de brecha y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.*



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/075/2024

- *Divulgar el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planemos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*
- *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

La prueba de daño precitada, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé que podrá considerarse como información reservada, aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad porque se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/075/2024

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 33 y 37 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda ..." (sic).

Establecidos los antecedentes del presente asunto, este Comité procede al análisis de los argumentos referidos con antelación, al tenor de las siguientes:

CONSIDERACIONES

PRIMERA. Con fundamento en lo dispuesto por los artículos 10 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, así como 8, fracción VI del Reglamento de Responsabilidades Administrativas de las y los Funcionarios y Empleados de la Universidad Nacional Autónoma de México, este Órgano Colegiado rige su funcionamiento, entre otros, bajo los principios de imparcialidad, certeza, legalidad, objetividad y profesionalismo. Por ello, al ser un asunto propuesto por la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, en este acto, su Titular e integrante de este Cuerpo Colegiado, Guadalupe Barrera Nájera, formalmente se excusa de conocer del caso, para no afectar la imparcialidad del mismo.

SEGUNDA. De conformidad con lo dispuesto en los artículos 1, 11 y 15, fracción X del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, el Comité de Transparencia de la Universidad Nacional Autónoma de México es competente para analizar la clasificación de reserva total de una parte de la información para la elaboración de la versión pública del Documento de Seguridad propuesta por la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, y determinar, en consecuencia, si la confirma, modifica o revoca.

TERCERA. De conformidad con lo dispuesto en los artículos 100 de la Ley General de Transparencia y Acceso a la Información Pública, 97 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 33 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, **los titulares de las Áreas Universitarias son responsables de clasificar la información que obre en sus archivos**, debiendo comunicar al Comité mediante oficio, de forma fundada y motivada, esa clasificación.

En tal virtud, la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género** clasificó como información reservada, por un periodo de **cinco años**, la relativa a los apartados correspondientes al **Análisis de Riesgo**, al **Análisis de Brecha** y al **Plan de Trabajo** de su Documento de Seguridad, conforme a lo expuesto en el antecedente VII de la presente resolución, por actualizarse el supuesto establecido en los artículos 113, fracción VII y 110, fracción VII de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente.



COMITÉ DE TRANSPARENCIA DE LA
UNIVERSIDAD NACIONAL AUTÓNOMA DE
MÉXICO

RESOLUCIÓN: CTUNAM/075/2024

Ahora bien, los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, establecen lo siguiente:

“... Como información reservada podrá clasificarse aquella cuya publicación:

[...]

VII. Obstruya la prevención o persecución de los delitos;

[...]”.

En correlación con los artículos antes mencionados, el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, establece los parámetros para la procedencia de la causal de reserva prevista en el artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública:

“Vigésimo sexto. De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, **aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.**

...”.

Énfasis añadido.

De lo anterior se desprende, entre otras cuestiones, que podrá clasificarse como reservada aquella información que obstruya la prevención de delitos, ya sea por obstaculizar las acciones implementadas por las autoridades para evitar la comisión de los mismos, o bien, por menoscabar o limitar su capacidad para evitarlos.

Al respecto, cabe tener en consideración lo establecido en el documento de trabajo del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal de la Organización de las Naciones Unidas, en el cual se define la prevención del delito de la siguiente manera: *“La prevención del delito engloba toda la labor realizada para reducir el riesgo de que se cometan delitos y sus efectos perjudiciales en las personas y la sociedad ...”.*

Por otro lado, las Directrices para la prevención del delito de la Organización de las Naciones Unidas enumeran tres enfoques, a saber, la prevención social, la prevención basada en la comunidad y la prevención de situaciones propicias al delito; este último tiene por objeto reducir las oportunidades y los incentivos para delinquir, maximizar el riesgo de ser aprehendido y reducir al mínimo los beneficios del delito. En este sentido, el enfoque de prevención de situaciones está orientada en formas específicas de delincuencia.



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/075/2024

Desde el punto de vista criminológico, prevenir implica conocer con anticipación la probabilidad de una conducta criminal disponiendo de los medios necesarios para evitarla. Es decir, no permitir que alguna situación llegue a darse cuando ésta se estima inconveniente.

Ahora bien, cabe destacar que conforme a las Directrices de la Organización para la Cooperación y el Desarrollo Económico, sobre protección de la privacidad y flujos transfronterizos de datos personales, los sectores público y privado, como principio básico, deben emplear salvaguardas razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos; asimismo, se establece el principio de responsabilidad que recae sobre todo controlador de datos y su deber en el cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

Asimismo, el artículo 7 del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, adoptado en Estrasburgo, Francia, el 28 de enero de 1981, publicado mediante Decreto de fecha 28 de septiembre de 2018 en el Diario Oficial de la Federación, establece que los Estados miembros deberán tomar medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados, contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Por su parte, el artículo 30, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, dispone como uno de los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en dicha Ley General, contar con un sistema de supervisión y vigilancia, interna y/o externa, incluidas auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

De igual forma, de conformidad con el artículo 33, fracción VII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el Sujeto Obligado deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, para lo cual en términos del numeral 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el responsable deberá monitorear, entre otras cuestiones, lo siguiente:

- Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
- Los incidentes y vulneraciones de seguridad ocurridas.

De conformidad con lo anterior, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, para establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/075/2024

personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, el responsable deberá monitorear y revisar de manera periódica dichas medidas, donde no podrán pasar inadvertidas las nuevas amenazas, las posibles vulnerabilidades, los riesgos en conjunto, los incidentes y las vulneraciones de seguridad ocurridas, entre otras.

En ese sentido, el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que los sujetos obligados deben elaborar un documento de seguridad, entendiéndose como tal, el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Ahora bien, de conformidad con los artículos 33 y 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en relación con los numerales 55 al 64 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el documento de seguridad deberá contener, cuando menos, el inventario de datos personales y de los sistemas de tratamiento; las funciones y obligaciones de las personas que traten datos personales; **el análisis de riesgos, el análisis de brecha, el plan de trabajo**, los mecanismos de monitoreo y revisión de las medidas de seguridad y el programa general de capacitación. Dicho documento deberá actualizarse cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio de nivel de riesgo; como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión; como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; así como con la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En tal orden de ideas, el segundo párrafo del artículo 5 de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, dispone que el documento de seguridad, deberá contener las medidas de seguridad administrativas, físicas y técnicas aplicables a los sistemas de tratamiento de datos personales de las Áreas Universitarias, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Además de lo anterior, de conformidad con el artículo 19, fracción I, incisos b) y c) de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, durante el tratamiento automatizado de los datos personales, los sistemas de información deberán establecer las medidas de seguridad en los periodos de inactividad o mantenimiento, así como generar respaldos y aplicar los mecanismos de control y protección para su resguardo.

Por ende, de difundirse la información contenida en los apartados relativos al **Análisis de Riesgos**, al **Análisis de Brecha**, al **Plan de Trabajo**, así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o que revele vulnerabilidades en la protección de los datos personales en poder del Área Universitaria**, se haría del conocimiento público la falta o debilidad de seguridad en un activo o grupo de activos, físicos o electrónicos, que puede ser explotada por una o más amenazas, lo que conllevaría a la materialización de las mismas y, derivado de ello, ocasionar la pérdida,



COMITÉ DE TRANSPARENCIA DE LA
UNIVERSIDAD NACIONAL AUTÓNOMA DE
MÉXICO

RESOLUCIÓN: CTUNAM/075/2024

destrucción no autorizada o incluso la sustracción de los datos personales en posesión de la Universidad, así como el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, además del daño, alteración o modificación no autorizada, incluso impidiendo su recuperación, vulnerando así la seguridad de los datos personales.

Bajo estos argumentos se advierte que la clasificación de la información contenida en el **Análisis de Riesgos**, en el **Análisis de Brecha**, en el **Plan de Trabajo**, así como de **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o que revele vulnerabilidades en la protección de los datos personales en poder del Área Universitaria**, tiene como propósito evitar o prevenir la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistemas de informática, la cual se encuentra prevista en el Título Noveno, Revelación de Secretos y Acceso Ilícito a sistemas y equipos de informática, Capítulo II, Acceso Ilícito a sistemas y equipos de informática, del Código Penal Federal en el cual se dispone lo siguiente:

“Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa”.

“Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

...”.

De la normativa señalada se advierte que comete el **delito de acceso ilícito a sistemas y equipos de informática** todo aquel que **sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sean o no propiedad del Estado**, o bien, conozca o copie dicha información; conductas que de igual manera se pueden materializar en los archivos físicos, ya que es factible **sustraer, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente, los datos personales contenidos en los documentos bajo custodia del Área Universitaria**, por lo que la misma protección deberá otorgarse tanto a los sistemas electrónicos, como a los archivos físicos con los que se cuenta.



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/075/2024

Por lo que de darse a conocer la información relativa al **Análisis de Riesgos**, al **Análisis de Brecha**, al **Plan de Trabajo**, así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder del Área Universitaria**, la cual se encuentra contenida en el Documento de Seguridad remitido por la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, se darían a conocer las acciones implementadas o por implementar, anticipando las medidas de seguridad más relevantes e inmediatas a establecer, así como las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser: hardware, software, personal responsable, manejo de documentos físicos y/o electrónicos, entre otros, lo que representa para el Área Universitaria un riesgo evidente para la estabilidad de la ejecución de las medidas de seguridad adoptadas para resguardar los datos en su poder, revelando elementos que, de manera concatenada con otra información que pudiera generarse o que se haya generado, evidenciaría vulnerabilidades que pudieran ser aprovechadas por personas dedicadas a la comisión de conductas ilícitas y con ello poner en riesgo la seguridad de los datos personales tratados en el desempeño y/o ejercicio de sus competencias, facultades y/o funciones.

De esta forma, se colige que con la publicidad de la información referida, se generaría un riesgo potencial tanto para la documentación física como para la infraestructura tecnológica del Área Universitaria, ya que la información relativa a las medidas físicas, administrativas y técnicas puede ser utilizada para propiciar, entre otros, actos vandálicos, o bien, ataques informáticos de diversa índole, al hacerse identificables las vulnerabilidades que pueden ser explotadas y causar un daño a los documentos físicos y/o electrónicos que obran en los archivos, así como a la infraestructura informática, programas y desarrollos tecnológicos del Área Universitaria, lo que limitaría severamente su capacidad para prevenir conductas ilícitas, tales como las relacionadas en párrafos anteriores.

Por lo anterior, se concluye que la información señalada actualiza la causal de reserva prevista en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como en el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Así, en términos del artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, se analiza la siguiente prueba de daño:

“Artículo 104. En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:

- I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;*
- II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y*
- III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio”.*



I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.

Difundir la información del Documento de Seguridad relativa al **análisis de riesgos**, al **análisis de brecha** y al **plan de trabajo**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder del Área Universitaria**, representa un riesgo potencial para el Área Universitaria, pues a través de dicha información se podrían identificar vulnerabilidades que pueden ser aprovechadas para realizar conductas contrarias a derecho, tales como actos vandálicos, o bien, ataques informáticos de diversa índole, disminuyendo la capacidad del Área Universitaria para responder ante posibles amenazas.

En ese sentido la divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.

II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda.

El perjuicio que en su caso ocasionaría la divulgación de la información en cuestión supera el perjuicio que se ocasionaría al no hacerla pública, pues con la difusión de la información contenida en el Documento de Seguridad relativa a los apartados de **análisis de riesgos**, de **análisis de brecha** y del **plan de trabajo**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder del Área Universitaria**, se limitaría su capacidad para prevenir la comisión de conductas ilícitas.

De ahí, resulta evidente que el riesgo de perjuicio que supondría la divulgación de la información solicitada, supera el interés público general de que se difunda.

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.

La limitación se ajusta al principio de proporcionalidad, toda vez que se justifica no difundir la información contenida en los apartados de **análisis de riesgos**, de **análisis de brecha** y del **plan de trabajo** del Documento de Seguridad, a cambio de garantizar la capacidad del Área Universitaria para implementar todas aquellas medidas y acciones tendientes a reducir el riesgo de que se cometa una conducta ilícita que pudiera vulnerar los datos personales cuyo tratamiento realizan con motivo del desempeño y/o ejercicio de sus competencias, facultades o funciones.

De igual manera, se considera que la limitación representa el medio menos restrictivo disponible para evitar el perjuicio, ya que únicamente se restringirá el acceso a la información por un periodo de **cinco años**, el cual fenecerá el **9 de febrero de 2029**, o bien, se interrumpirá antes si desaparecen las causas que originaron la reserva de la información, lo que suceda primero; pues durante dicho periodo podría tener lugar alguna modificación sustancial o una actualización del Documento de Seguridad.



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/075/2024

De tal forma que no se afecte la capacidad de este sujeto obligado para prevenir la comisión de conductas ilícitas, pero tampoco se prive de manera trascendente el acceso a la información, ya que éste no se verá restringido por un periodo mayor al establecido en esta resolución, el cual es acorde con lo previsto por la norma.

Por lo antes mencionado, se colman las hipótesis de las fracciones I, II y III del artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, por lo que es procedente **CONFIRMAR** la reserva parcial de la información para la elaboración de la versión pública propuesta por la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, por un periodo de **cinco años**, que se computará a partir de la fecha de la presente resolución, de conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

CUARTA. La **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género** deberá verificar que su Documento de Seguridad cuente y cumpla con la información y características establecidas en cada uno de los apartados y sub apartados del “Anexo I. Documento de Seguridad de Datos Personales” de los “Anexos de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad”, aprobados por este Cuerpo Colegiado mediante Acuerdo de fecha 10 de enero de 2020.

De advertir que es necesario complementar, modificar y/o actualizar el contenido sustancial de su Documento de Seguridad, en todo o en parte, deberá elaborar nuevamente la versión pública correspondiente y someterla a consideración de este Comité para los efectos conducentes, en términos de lo establecido en los artículos precisados en el primer párrafo de la consideración **TERCERA** de la presente resolución.

QUINTA. La **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género** elaborará la versión pública de su Documento de Seguridad, teniendo en cuenta lo siguiente:

- Testar las secciones o información correspondientes al “Análisis de Riesgo”, al “Análisis de Brecha”, al “Plan de Trabajo”, así como toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en su poder; para lo cual emplearán un medio que no permita la visualización de la misma y que no impida la lectura de aquella información que no es considerada como reservada. Al respecto, es importante precisar que **no deberán suprimirse las secciones** donde se contenga la información objeto de reserva.
- Insertar un cuadro de texto en el cual se indiquen:
 - Las partes o secciones reservadas.
 - El fundamento legal que sustenta la reserva, así como el plazo de ésta, mismos que se encuentran indicados en el último párrafo de la consideración **TERCERA** de la presente resolución.



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/075/2024

Lo anterior, de conformidad con lo dispuesto en los numerales Quincuagésimo Segundo, Quincuagésimo Tercero, Quincuagésimo Octavo, Quincuagésimo Noveno, Sexagésimo y Sexagésimo Primero de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Por lo expuesto, y con fundamento en lo dispuesto por los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 1, 6, 7, 8, 23, 44, fracción II, 106, fracción II, 113, fracción VII, 137, inciso a) de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 98, fracción II, 110, fracción VII, y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública; 1, 15, fracción X, 34 fracción II y 42, primer párrafo del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, este Comité de Transparencia:

RESUELVE

PRIMERO. Con fundamento en lo dispuesto por los artículos 1, 10, 11, 15 fracción X y 42, primer párrafo del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, 137, inciso a) de la Ley General de Transparencia y Acceso a la Información Pública y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia **CONFIRMA** la **CLASIFICACIÓN de RESERVA** parcial de la información para la elaboración de la versión pública propuesta por la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, en relación con los apartados de **Análisis de Riesgos**, de **Análisis de Brecha** y del **Plan de Trabajo**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder del Área Universitaria**, contenida en su Documento de Seguridad, por un periodo de **cinco años**, contados a partir de la fecha de la presente resolución.

Lo anterior, en términos de la consideración **TERCERA** de la presente resolución.

SEGUNDO. Se instruye a la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, a fin de que verifique que su Documento de Seguridad contenga la información requerida y reúna las características establecidas en la normativa universitaria aplicable y, de ser el caso, someta nuevamente a este Cuerpo Colegiado la clasificación correspondiente, de acuerdo con lo señalado en la consideración **CUARTA** de esta resolución.

TERCERO. Se instruye a la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género** a efecto de que elabore la versión pública en términos de lo dispuesto en la consideración **QUINTA**.

CUARTO. Con fundamento en los artículos 45, fracción V y 137, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública; así como 42 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, notifíquese la presente resolución por correo institucional a la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, así como a la Unidad de Transparencia de esta Universidad, para los efectos procedentes.



COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/075/2024

Así lo resolvió por unanimidad de votos de sus integrantes, el Comité de Transparencia de la Universidad Nacional Autónoma de México, en términos de los artículos 1, 11, 15, 19 y 42 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

**“POR MI RAZA HABLARÁ EL ESPÍRITU”
Ciudad Universitaria, Cd. Mx., a 9 de febrero de 2024**

Archivo

Identificador único (hash)

Fecha y hora de cierre

Número de páginas

13-ctunam-075-2024-docto-seg-8.pdf

998ccb9c1033d38000cf80af2049ddf4948c9440bb6cba0ea8de94e99cc8a1cb

09/02/2024 21:54:20

14

Fecha y hora de emisión

Firmantes

09/02/2024 22:00:55

5



Firmantes

Nombre	Dra. Susana Conrada Alva Chimal	Fecha y hora de firma	09/02/2024 17:07:57
Dirección General de Responsabilidades, Inconformidades, Quejas y Registro Patrimonial y Suplente del Contralor			
Hash Firma	fbe15aef8c6a628285a52383bbb3277c0b44b47637cda6110085ad0cf0e39ef76d01b37cb220582ca61381dd9b6aaf01		

Nombre	Lic. Porfirio Antonio Diaz Rodríguez	Fecha y hora de firma	09/02/2024 17:17:44
Titular de la Dirección General de Servicios Generales y Movilidad			
Hash Firma	2366a5c96c1abcf8352d001b8874918ed4b7ed18d69c242f3fd0a9eacbb87814bc9da783cb3df6dc71e6e51d5c16e8b0		

Nombre	Dr. José Meljem Moctezuma	Fecha y hora de firma	09/02/2024 16:56:46
Titular de la Unidad de Transparencia			
Hash Firma	95acb947fd507e3ca62df491815188da7a68c81d6d0b21f2077c86f203c3ad5028678c75dff1fc5e88e0d3137726666a		

Nombre	Dra. Jacqueline Peschard Mariscal	Fecha y hora de firma	09/02/2024 15:59:59
Especialista			
Hash Firma	3df2be2d32ceae184fafc13f39cd47545a87892226ba49c2e3ab9031699b504ca7416dfe45e769dfd2a844b94f9c5a8c		

Nombre	Dra. Angela Quiroga Quiroga	Fecha y hora de firma	09/02/2024 21:54:20
Directora General de Estudios de Legislación Universitaria y Suplente del Presidente del Comité de Transparencia			
Hash Firma	e7fdcf798b365ab6738538b68c68adccfb2915ce3b0431b0b721916d361f4c1da661cf1cf2e88642c696dd24c2cb1f6e		