Documento de Seguridad de Datos Personales

Dirección General de Estudios de Legislación Universitaria

Agosto del 2022

Dirección General de Estudios de Legislación Universitaria

DIRECCIÓN GENERAL DE ESTUDIOS DE LEGISLACIÓN UNIVERSITARIA

[redacted]DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES[redacted]

ÍNDICE

Introducción

El presente documento de seguridad contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales del 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*".

Objetivos

Describir las medidas de seguridad del Sistema de Gestión de la Seguridad de Datos Personales de la Dirección General de Estudios de Legislación Universitaria (DGELU), desde su obtención, uso, registro, organización, estructuración, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión o cualquier otra forma de habilitación de acceso, cotejo, interconexión, manejo, aprovechamiento, divulgación, transferencia, supresión, destrucción o disposición de datos personales, así como proteger todos los datos y datos personales sensibles que se recaben y de accesos no autorizados ni de tratamientos distintos a los fines para los que fueron recabados, mediante cualquiera de los siguientes tipos de soporte: en soportes físicos, en soportes electrónicos y en redes de datos.

Definiciones

I. **Bases de datos**: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

II. **Borrado seguro**: Procedimiento para la eliminación en un dispositivo o medio de almacenamiento, conocido o por conocer, que impide la recuperación de los datos personales.

III. **Confidencialidad**: Es el principio de seguridad de la información que consiste en que la información no pueda estar disponible o divulgarse a personas o procesos no autorizados por el Área Universitaria respectiva.

IV. **DGTIC**: Dirección General de Tecnologías de la Información y Comunicación.

V. **Documento de seguridad**: 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.

VI. **Encargado**: La persona física o jurídica distinta a las áreas, entidades o dependencias universitarias, que realizan el tratamiento de los datos personales a nombre de la Universidad, suscribiendo para tal efecto los instrumentos consensuales correspondientes acordes con la Legislación Universitaria aplicable.

VII. **Medidas de seguridad**: Conjunto de acciones, actividades, controles o mecanismos técnicos, administrativos y físicos que permitan proteger los datos personales.

VIII. **Medidas de seguridad físicas**: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, los cuales pueden ser desde medidas preventivas, cotidianas y correctivas para tener un control de acceso, preservación, conservación de las instalaciones, recursos o bienes en los cuales se resguarda información e incluso a la información misma, asegurando así su disponibilidad e integridad. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

IX. **Medidas de seguridad técnicas**: Conjunto de acciones y mecanismos para proteger los datos personales que se encuentren en formato digital, así como los sistemas informáticos que les den tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Asegurar que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario realice las actividades que requiere con motivo de sus funciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

X. **Nube institucional**: Modelo de servicios de tecnología de información proporcionados bajo demanda a las áreas universitarias, en infraestructura propiedad de la universidad y que incluye cómputo, almacenamiento, plataforma, seguridad y respaldos.

XI. **Principio del menor privilegio**: Otorgamiento de los permisos necesarios y suficientes a un usuario autorizado para acceder a un sistema de información para el desempeño de sus actividades.

XII. **Red de datos**: Conjunto de componentes electrónicos activos y medios de comunicación conocidos o por conocer tales como fibra óptica, enlaces inalámbricos, cable, entre otros, que permiten el intercambio de paquetes de datos entre dispositivos electrónicos para el procesamiento de información.

XIII. **Responsable**: Las Áreas Universitarias que manejan, resguardan y/o deciden sobre el tratamiento de datos personales.

XIV. **Soporte**: Medio, ya sea electrónico o físico, en el que se registra y guarda información, como lo es: el papel, así como los audiovisuales, fotográficos, fílmicos, digitales, electrónicos, sonoros y visuales, entre otros, y los que produzca el avance de la tecnología.

XV. **Soportes electrónicos**: Son los medios de almacenamiento accesibles sólo a través del uso de algún dispositivo electrónico conocido o por conocer, que procese su contenido para examinar, modificar o almacenar los datos; tales como cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs, DVDs y Blue-rays), discos magneto ópticos, discos magnéticos (flexibles y duros) y demás medios para almacenamiento masivo no volátil.

XVI. **Soportes físicos**: Son los medios de almacenamiento accesibles de forma directa y sin intervención de algún dispositivo para examinar, modificar o almacenar los datos; tales como documentos, oficios, formularios impresos, escritos autógrafos, documentos de máquina de escribir, fotografías, placas radiológicas, carpetas, expedientes, entre otros.

XVII. **Transferencia**: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del Responsable o del Encargado.

XVIII. **Tratamiento**: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)	
Identificador único*	SAGICO
(Nombre del sistema A1) *	Sistema para la Administración y Gestión de Instrumentos Consensuales
Datos personales (sensibles o no) contenidos en el sistema*:	Los datos personales son los que están contenidos en los instrumentos consensuales almacenados en el SAGICO. Nombres completos de los involucrados, firmas autógrafas, firmas electrónicas, domicilios, cargos, números de trabajador. No hay datos sensibles.
Responsable*:	
Nombre*:	**Mtro. Hans Kohler Lizardi**
Cargo*:	**Jefe de la Unidad de Informática de la Oficina de la Abogacía General**
Funciones*:	Recibir y dar trámite a las solicitudes de acceso al SAGICO. Consultar la información y generar los reportes que le soliciten las instancias universitarias. Notificar a los solicitantes los nombres de usuarios y contraseñas de acceso al SAGICO.
Obligaciones*:	Mejorar la funcionalidad en cuanto a la seguridad del sistema para garantizar la protección de los datos personales. Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Proteger la integridad del SAGICO ante posibles riesgos que alteren su funcionalidad. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
Encargados:	
(Nombre del Encargado 1*)	**Lic. Rafael González Zaldivar**
Cargo*:	**Director de Documentación y Difusión**
Funciones*:	Gestionar la generación de los reportes que le soliciten las diferentes áreas internas de la DGELU, así como instancias universitarias. Recibir y dar trámite a las solicitudes para el acceso al SAGICO. Notificar a los solicitantes los nombres de usuarios y contraseñas de acceso al SAGICO.

Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Proteger la integridad del SAGICO ante posibles riesgos que alteren su funcionalidad.
(Nombre del Encargado 2*)	**Ing. Dulce María Milián García**
Cargo*:	**Jefa del Departamento de Cómputo y Automatización de la DGELU**
Funciones*:	Consultar la información y generar los reportes que le soliciten las áreas internas de la DGELU. Generar los nombres de usuario y contraseñas para el acceso al SAGICO. Realizar las correcciones de los datos de identificación de los instrumentos consensuales, cuando sea necesario. Realizar diariamente el respaldo de la base de datos del SAGICO. Apoyar en la corrección del código de programación del SAGICO, cuando sea solicitado. A petición de las áreas de la DGELU y previa autorización, eliminar registros de la base de datos del SAGICO. Brindar asesorías con relación a la utilización del SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Proteger la integridad del SAGICO ante posibles riesgos que alteren su funcionalidad. Mantener en funcionamiento constante el servidor donde se aloja el SAGICO. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Encargado 3*)	Ing. David Ricardo Montalván Rodríguez
Cargo*:	**Asistente de Procesos**
Funciones*:	Consultar la información y generar los reportes que le soliciten las áreas internas de la DGELU, así como instancias universitarias. Realizar las correcciones de los datos de identificación de los instrumentos consensuales, cuando sea necesario. Realizar diariamente el respaldo de la base de datos del SAGICO. A petición de las áreas de la DGELU y previa autorización, eliminar registros de la base de datos del SAGICO. Brindar asesorías con relación a la utilización del SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los

	instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Proteger la integridad del SAGICO ante posibles riesgos que alteren su funcionalidad. Mantener en funcionamiento constante el servidor donde se aloja el SAGICO. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
Usuarios:	
Dirección General	
(Nombre del Usuario 1*)	Dr. Daniel Márquez Gómez
Cargo*:	**Director General de Estudios de Legislación Universitaria**
Funciones*:	Consultar los instrumentos consensuales almacenados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales.
(Nombre del Usuario 2*)	Lic. José Abraham González Becerra
Cargo*:	**Coordinador de Gestión**
Funciones*:	Coordinar la entrada, dar seguimiento y desahogo de los instrumentos consensuales contenidos en el SAGICO, de conformidad con la Legislación Universitaria. Consultar y generar reportes de los instrumentos consensuales almacenados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales.
Dirección de Convenios	
(Nombre del Usuario 1*)	Mtro. Luis Leopoldo Hidalgo García
Cargo*:	**Director**
Funciones*:	Coordinar la entrada, seguimiento y desahogo de los instrumentos consensuales (convenios), de conformidad con la Legislación Universitaria. Consultar y generar reportes de los instrumentos consensuales almacenados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales.

	No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 2*)	Karla Gabriela Hernández Andrade
Cargo*:	**Jefa del Departamento de Instrumentos Consensuales Nacionales**
Funciones*:	Realizar el seguimiento, consulta de antecedentes y control de los instrumentos consensuales asignados al área de Convenios. Consultar, analizar y generar reportes de los instrumentos consensuales almacenados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 3*)	Cristina Galicia Vázquez
Cargo*:	**Jefa del Departamento de Instrumentos Consensuales Internacionales**
Funciones*:	Realizar el seguimiento, consulta de antecedentes y control de los instrumentos consensuales asignados al área de Convenios. Consultar, analizar y generar reportes de los instrumentos consensuales almacenados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 4*)	Erika Alejandra Suárez Guevara
Cargo*:	**Secretaria Auxiliar**
Funciones*:	Consultar, capturar, turnar, dar seguimiento, realizar análisis y editar la información de identificación de los instrumentos consensuales alojados en el SAGICO. Administrar los datos de las "contrapartes" señaladas en los instrumentos consensuales. Intercambiar y verificar información con la Dirección de

	Apoyo Normativo a Comités y Contratos.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 5*)	Rosa María Mercado Corona
Cargo*:	**Asistente ejecutiva**
Funciones*:	Consultar, capturar, dar seguimiento, realizar análisis de los instrumentos consensuales alojados en el SAGICO. Administrar los datos de las "contrapartes" señaladas en los instrumentos consensuales.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 6*)	Miguel Ángel Cabrera Rojas
Cargo*:	**Abogado Auxiliar**
Funciones*:	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 7*)	Citlalminani Pérez Montoya
Cargo*:	**Abogada Auxiliar**
Funciones*:	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los

	instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 8*)	Karla Itzamara Eslava Méndez
Cargo*:	**Abogada Auxiliar**
Funciones*:	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 9*)	Marco Antonio Núñez Campuzano
Cargo*:	**Abogado Auxiliar**
Funciones*:	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 10*)	María Estela López Pérez
Cargo*:	**Abogada Auxiliar**
Funciones*:	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor

	de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 11*)	Eleazar Albarrán Vergara
Cargo*:	**Abogado Auxiliar**
Funciones*:	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 12*)	Emmanuel Coraza Pérez
Cargo*:	**Abogado Auxiliar**
Funciones*:	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 13*)	María Alejandra Sánchez Vite
Cargo*:	**Abogada Auxiliar**
Funciones*:	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 14*)	Soledad Iliana Orihuela Aguilar

Cargo*:	**Abogada Auxiliar**
Funciones*:	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 15*)	Lizbet Guadalupe Flores Gómez
Cargo*:	**Abogada Auxiliar**
Funciones*:	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
Dirección de Apoyo Normativo a Comités y Contratos	
(Nombre del Usuario 1*)	Lic. Alejandro Martínez Tapia
Cargo*:	**Director**
Funciones*:	Coordinar la entrada, seguimiento y desahogo de los instrumentos consensuales de contratos, contratos y convenios en materia de obras, de conformidad con la Legislación Universitaria. Consultar y generar reportes de los instrumentos consensuales almacenados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 2*)	Alejandro César Arzate Villanueva
Cargo*:	**Jefe del Departamento de Apoyo Normativo a**

	Adquisiciones
Funciones*:	Realizar la captura, edición, análisis, seguimiento, asignación y consulta de instrumentos consensuales de contratos.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 3*)	Palemón Albarrán Arce
Cargo*:	**Jefe del Departamento de Apoyo Normativo a Obras**
Funciones*:	Realizar el análisis y consulta de antecedentes de instrumentos consensuales de contratos y convenios en materia de obras.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 4*)	Roberto Campos Carreón
Cargo*:	**Abogado Auxiliar**
Funciones*:	Analizar, buscar, realizar consultas de antecedentes, generar reportes, capturar los instrumentos consensuales.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 5*)	Gilberto Zambrano Mar
Cargo*:	**Secretario Auxiliar**
Funciones*:	Analizar, buscar, realizar consultas de antecedentes, generar reportes, capturar los instrumentos consensuales.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los

	instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 6*)	Alfredo Velasco Valerio
Cargo*:	**Abogado Auxiliar**
Funciones*:	Analizar, buscar, realizar consultas de antecedentes, generar reportes, capturar los instrumentos consensuales.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 7*)	Elvia Lucía Flores Ávalos
Cargo*:	**Abogada Auxiliar**
Funciones*:	Analizar, buscar, realizar consultas de antecedentes, generar reportes, capturar los instrumentos consensuales.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
(Nombre del Usuario 8*)	Karla Pamela Cabrera Sánchez
Cargo*:	**Abogada Auxiliar**
Funciones*:	Analizar, buscar, realizar consultas de antecedentes, generar reportes, capturar los instrumentos consensuales.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.

(Nombre del Usuario 9*)	Adriana López Trinidad
Cargo*:	**Asistente ejecutiva**
Funciones*:	Analizar, buscar, realizar consultas de antecedentes, generar reportes, capturar los instrumentos consensuales. Administrar los datos de las "contrapartes" señaladas en los instrumentos consensuales. Intercambiar y verificar información con la Dirección de Convenios.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Mantener las versiones definitivas de los instrumentos consensuales que contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
Departamento de Enlace de Transparencia	
(Nombre del Usuario 1*)	Vacante
Cargo*:	**Jefe de Departamento**
Funciones*:	Consultar los instrumentos consensuales almacenados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales.
(Nombre del Usuario 2*)	Isabel Molina Cigarroa
Cargo*:	**Abogada Auxiliar**
Funciones*:	Consultar los instrumentos consensuales almacenados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales.
(Nombre del Usuario 3*)	Marisol Guevara Arteaga
Cargo*:	**Abogada Auxiliar**
Funciones*:	Consultar los instrumentos consensuales almacenados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos

	en los instrumentos consensuales.
(Nombre del Usuario 4*)	Luz Ofelia Sobrado Ramírez
Cargo*:	**Abogada Auxiliar**
Funciones*:	Consultar los instrumentos consensuales almacenados en el SAGICO.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales.
379 Usuarios solicitantes web	
Cargo*:	**Responsables, encargados, designados por el titular de las entidades o dependencias universitarias o cualquier otra persona que tenga los permisos correspondientes para desarrollar dichas actividades.**
Funciones*:	Consultar, dar seguimiento, generar reportes y/o capturar los instrumentos consensuales en el SAGICO de sus respectivas entidades y dependencias.
Obligaciones*:	Proteger los datos personales de los involucrados en los instrumentos consensuales, no modificarlos, no difundirlos, no realizar alteraciones deliberadamente.

Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General	
Identificador único*	Usuarios
(Nombre del sistema A2) *	Biblioteca "Jorge Carpizo"
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de identificación: Nombre, celular personal, correo electrónico personal. Datos laborales: puesto, correo electrónico institucional, teléfono institucional y lugar donde labora. No hay datos sensibles.
Responsable*:	
Nombre*:	**Ing. Jesús Antonio Sandoval Navarrete**
Cargo*:	**Responsable de la Biblioteca**
Funciones*:	Administrar la base de datos de usuarios.
Obligaciones*:	Proteger los datos de los usuarios, almacenarlos en lugar seguro, realizar respaldos periódicamente, conservar la base, guardar en todo momento la confidencialidad del contenido de los datos.

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria	
Identificador único*	SAP
(Nombre del sistema A3) *	Sistema Almacén de Publicaciones
Datos personales (sensibles o no) contenidos en el sistema*:	Los datos personales son los solicitados para generar el recibo de dotación (venta o donación): Nombre, cargo, dependencia, domicilio, teléfono institucional o personal,

	correo electrónico institucional o personal, nombre de quien autoriza, nombre de quien elabora el recibo, nombre de quien recibe la publicación. No hay datos sensibles.
Responsable*:	
Nombre*:	**Ing. Jesús Antonio Sandoval Navarrete**
Cargo*:	**Jefe del Departamento de Publicaciones**
Funciones*:	Consultar la base de datos, capturar los datos del cliente, generar el recibo de dotación, recabar la firma de autorización y entregar la publicación.
Obligaciones*:	Proteger los datos de los clientes, resguardar los datos en lugar seguro, realizar respaldos periódicamente, guardar en todo momento la confidencialidad del contenido de los datos.

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

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)	
Identificador único*	SAGICO
(Nombre del sistema A1*)	Sistema para la Administración y Gestión de Instrumentos Consensuales
Tipo de soporte:*	Físico y Electrónico
Descripción:*	Base de datos. Expedientes.
Características del lugar donde se resguardan los soportes:*	Servidor de datos. ver comentario

Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General	
Identificador único*	Usuarios
(Nombre del sistema A2*)	Biblioteca "Jorge Carpizo"
Tipo de soporte:*	Físico y electrónico.
Descripción:*	ver comentario
Características del lugar donde se resguardan los soportes:*	Soporte físico: En carpeta de argollas en la biblioteca, el acceso se encuentra limitado y bajo el resguardo del responsable de la biblioteca. Soporte electrónico: Equipo de cómputo del responsable de la biblioteca, No. de inventario: 02309919, como medida de seguridad, se estableció un nombre de usuario y una contraseña para ingresar a la información del equipo, no se tiene acceso desde la red.

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria	
Identificador único*	SAP
(Nombre del sistema A3*)	Sistema Almacén de Publicaciones
Tipo de soporte:*	Físico y electrónico.

Eliminado: dos renglones en donde se especifican las características del lugar donde se resguardan los soportes y un reglón, relacionado con la descripción de soporte. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

Descripción:*	ver comentario
Características del lugar donde se resguardan los soportes:*	Soporte físico: En carpeta de argollas en el Almacén de Publicaciones, el acceso se encuentra limitado mediante puerta con doble cerradura. Soporte electrónico: En equipo de cómputo del Jefe de Departamento, No. de inventario: 02309919, con nombre de usuario y contraseña como medida de seguridad, no se tiene acceso a la base de datos desde la red.

3. ANÁLISIS DE RIESGOS

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)		
Identificador único*	SAGICO	
(Nombre del sistema A1) *	Sistema para la Administración y Gestión de Instrumentos Consensuales	
Riesgo*	**Impacto***	**Mitigación***
ver comentario		
ver comentario		
ver comentario		
ver comentario		

Eliminado: un reglón, relacionado con la descripción de soporte y doce cuadros con descripción correspondientes al Análisis de Riesgo. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

		ver comentario

ver comentario

ver comentario

ver comentario

ver comentario

ver comentario

ver comentario

Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General		
Identificador único*	Usuarios	
(Nombre del sistema A2) *	Biblioteca "Jorge Carpizo"	
Riesgo*	**Impacto***	**Mitigación***

ver comentario

Eliminado: veinticinco cuadros con descripción correspondientes al Análisis de Riesgo. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

	ver comentario

ver comentario

ver comentario

ver comentario

ver comentario

ver comentario

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria		
Identificador único*	SAP	
(Nombre del sistema A3) *	Sistema Almacén de Publicaciones	
Riesgo*	**Impacto***	**Mitigación***

ver comentario

ver comentario

ver comentario

ver comentario

Eliminado: veintinueve cuadros con descripción correspondientes al Análisis de Riesgo. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

		ver comentario

ver comentario

ver comentario

4. ANÁLISIS DE BRECHA

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)		
Identificador único*	SAGICO	
(Nombre del sistema A1) *	Sistema para la Administración y Gestión de Instrumentos Consensuales	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***

ver comentario

ver comentario

Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General

Eliminado: un renglón y doce cuadros con descripción correspondiente al Análisis de Riesgo y seis cuadros con descripción correspondientes al Análisis de Brecha. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

Identificador único*	Usuarios	
(Nombre del sistema A2) *	Biblioteca "Jorge Carpizo"	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
ver comentario		
ver comentario		

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria		
Identificador único*	SAP	
(Nombre del sistema A3) *	Sistema Almacén de Publicaciones	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
ver comentario		
ver comentario		

5. PLAN DE TRABAJO

ver comentario

[redacted]

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección

Eliminado: doce cuadros con descripción correspondientes al Análisis de Riesgo y seis renglones correspondientes al Plan de Trabajo. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

General de Estudios de Legislación Universitaria (DGELU)			
Identificador único*	SAGICO		
(Nombre del sistema A1) *	Sistema para la Administración y Gestión de Instrumentos Consensuales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
ver comentario			
ver comentario			
ver comentario			
ver comentario			

Eliminado: dieciséis cuadros con descripción correspondientes al Plan de Trabajo. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

ver comentario

ver comentario

ver comentario

Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General			
Identificador único*	Usuarios		
(Nombre del sistema A2) *	Biblioteca "Jorge Carpizo"		
Actividad*	**Descripción***	**Duración***	**Cobertura***

ver comentario

ver comentario

ver comentario

	ver comentario		ver comentario

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria			
Identificador único*	SAP		
(Nombre del sistema A3) *	Sistema Almacén de Publicaciones		
Actividad*	**Descripción***	**Duración***	**Cobertura***
ver comentario			
ver comentario			
ver comentario			

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)	
Identificador único*	*SAGICO*

Eliminado: catorce cuadros con descripción correspondientes al Plan de Trabajo. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

(Nombre del sistema A1)*	*Sistema para la Administración y Gestión de Instrumentos Consensuales*
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales en soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales en soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales sobre redes electrónicas.

Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General	
Identificador único*	Usuarios
(Nombre del sistema A2)*	Biblioteca "Jorge Carpizo"
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales en soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales en soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales sobre redes electrónicas.

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria	
Identificador único*	SAP
(Nombre del sistema A3)*	Sistema Almacén de Publicaciones
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias de datos personales en soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias de datos personales en soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	No se realizan transferencias de datos personales sobre redes electrónicas.

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

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)	
Identificador único*	SAGICO
(Nombre del sistema A1)*	Sistema para la Administración y Gestión de Instrumentos Consensuales

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

ver comentario

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

Ver Anexo 1.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   b) Para soportes físicos: Número o clave del expediente utilizado, y
   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
   Para soporte físico, la Dirección de Convenios posee bitácoras de acceso y uso cotidiano en sus expedientes, las cuales contienen: número de registro, hora de acceso al expediente, fecha de salida, fecha de devolución y nombre y firma del solicitante.
2. Si las bitácoras están en soporte físico o en soporte electrónico;
   Se encuentran en soporte electrónico y soporte físico (solo para la Dirección de Convenios).
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
   Para soporte electrónico, se almacenan en el mismo sistema y de forma permanente. En la Dirección de Convenios, las bitácoras se almacenan en cada expediente.
4. La manera en que asegura la integridad de las bitácoras, y
   Para soporte electrónico, por la seguridad en el mismo sistema y del centro de datos de la DGELU. En la Dirección de Convenios se asegura que cada bitácora preserve su integridad con el expediente mismo.
5. Respecto del análisis de las bitácoras:

Eliminado: once renglones con descripción correspondientes al Resguardo de Sistemas de Tratamiento de Datos Personales con Soportes Físicos. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y

Para soporte electrónico, el análisis se efectúa por la Jefa del Departamento de Cómputo y Automatización de la DGELU, cada vez que hay modificaciones al sistema. Para soporte físico, en la Dirección de Convenios, las bitácoras son analizadas, según sea el caso, por las Jefas de Departamento y/o por el Director de Convenios.

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

ver comentario

IV. REGISTRO DE INCIDENTES:

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

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) La metodología aplicada;
   c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
   d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

Para la pérdida o alteración no autorizada de expedientes en soportes físicos y electrónicos se levanta el acta administrativa correspondiente ante el titular de la DGELU, donde se consignen las situaciones de modo, tiempo y lugar y haga constar los hechos que se describen, para remitir a las instancias competentes.

V. ACCESO A LAS INSTALACIONES

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

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

Para el control de acceso a las instalaciones de la DGELU, se cuenta con dos puntos de control las 24 horas, mediante control biométrico, operado por la Unidad Administrativa de la dependencia. También se cuenta con un sistema de video vigilancia las 24 horas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?

Eliminado: un renglón con descripción correspondiente al Bitácoras para Acceso y Operación Cotidiana. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

Para personas que laboran en la DGELU, se identifican mediante el reconocimiento facial y/o la huella dactilar (control biométrico).

Para personas ajenas a la dependencia, el personal interno atiende a las personas y pregunta e identifica el tipo de trámite que desean realizar en la DGELU, con base en las funciones, atribuciones y competencias de la dependencia.

b) ¿Cómo las autentifica?

Para personas que laboran en la DGELU, mediante la comprobación de los elementos descritos en el inciso a) con los almacenados en la base de datos del control de acceso.

Para personas ajenas a la dependencia, con la credencial de la UNAM, con credencial para votar con fotografía, con licencia de conducir u otra identificación que demuestre su identidad.

c) ¿Cómo les autoriza el acceso?

Para personas que laboran en la DGELU, después de identificar y autenticar al personal, se permite el acceso automáticamente.

Para personas ajenas a la dependencia: después de identificar y autenticar a la personal, se permite el acceso automáticamente.

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

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

Soportes físicos o electrónicos: Para la seguridad perimetral interior se cuenta con acceso a los espacios mediante puertas y cerraduras bajo llave. La administración de las llaves está a cargo de la Unidad Administrativa y cada usuario tiene su propia llave de acceso, cuando así sea el caso. Se cuenta con un sistema de tratamiento de datos personales mediante video vigilancia y control biométrico las 24 horas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Por ser trabajador de la DGELU, previamente registrado en el control de acceso biométrico bajo la autorización de la Unidad Administrativa de la DGELU.
2. ¿Cómo las autentifica?
   Mediante control biométrico.
3. ¿Cómo les autoriza el acceso?
   Mediante acceso automático.

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

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

Mediante correo electrónico institucional se solicita la actualización de los datos personales contenidos en sistema, conforme a los requerimientos y responsabilidades de cada área solicitante.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):
- **a)** ¿Está basado en roles (perfiles) o grupos?
  Si.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
  No aplica.
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
  No aplica.
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  No aplica.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
  Si.

[redacted] ver comentario [redacted]

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles?
  La Jefa del Departamento de Cómputo y Automatización de la DGELU o el Encargado del SAGICO.
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
  El Director de Documentación y Difusión.
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?
  Si, se encuentran contenidos en la base de datos de sistema.

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

[redacted] ver comentario [redacted]

Eliminado: once renglones con descripción correspondientes al Perfiles de Usuario y Contraseñas. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos__x__, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual __x__,
   c) Periodicidad con que los realiza: diariamente y mensualmente.
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad
   Disco duro.

[redacted] ver comentario [redacted]

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

IX. PLAN DE CONTINGENCIA

[redacted] ver comentario [redacted]

[redacted] ver comentario [redacted]

Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General	
Identificador único*	Usuarios
(Nombre del sistema A2)*	Biblioteca "Jorge Carpizo"

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

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

[redacted] ver comentario [redacted]

Eliminado: dos renglones con descripción correspondientes al Procedimiento de Respaldo y Recuperación de Datos y dieciséis renglones correspondientes al Plan de Contingencia y dos renglones correspondientes al Resguardo de Sistemas de Tratamiento de Datos Personales con Soporte Físico. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

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

Nombre	Cargo	Funciones	Obligaciones
Jesús Antonio Sandoval Navarrete	Responsable de Biblioteca	Administrar la base datos de usuarios	Proteger los datos de los usuarios, almacenarlos en lugar seguro, realizar respaldos periódicamente, conservar la base, guardar en todo momento la confidencialidad del contenido de los datos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**

   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   b) Para soportes físicos: Número o clave del expediente utilizado, y
   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
6. Si las bitácoras están en soporte físico o en soporte electrónico;
7. Lugar dónde almacena las bitácoras y por cuánto tiempo;
8. La manera en que asegura la integridad de las bitácoras, y
9. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

El Responsable de la Biblioteca es quien tiene el acceso a los datos personales para el funcionamiento de la propia Biblioteca.

IV. REGISTRO DE INCIDENTES:

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

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) La metodología aplicada;
   c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
   d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

Para la pérdida o alteración no autorizada de expedientes en soportes físicos y electrónicos se levanta

el acta administrativa correspondiente ante el titular de la DGELU, donde se consignen las situaciones de modo, tiempo y lugar y haga constar los hechos que se describen, para remitir a las instancias competentes.

V. ACCESO A LAS INSTALACIONES

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

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

Para el control de acceso a las instalaciones de la DGELU, se cuenta con dos puntos de acceso funcionando las 24 horas, operado por la Unidad Administrativa de la dependencia. También se cuenta con un sistema de video vigilancia las 24 horas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
   Para personas que laboran en la DGELU, se identifican mediante el reconocimiento facial y/o la huella dactilar (control biométrico).
   Para personas ajenas a la dependencia, el personal interno atiende a las personas y pregunta e identifica el tipo de trámite que desean realizar en la DGELU, con base en las funciones, atribuciones y competencias de la dependencia.
b) ¿Cómo las autentifica?
   Para personas que laboran en la DGELU, mediante la comprobación de los elementos descritos en el inciso a) con los almacenados en la base de datos del control de acceso.
   Para personas ajenas a la dependencia, con la credencial de la UNAM, con credencial para votar con fotografía, con licencia de conducir u otra identificación que demuestre su identidad.
c) ¿Cómo les autoriza el acceso?
   Para personas que laboran en la DGELU, después de identificar y autenticar al personal, se permite el acceso automáticamente.
   Para personas ajenas a la dependencia: después de identificar y autenticar a la personal, se permite el acceso automáticamente.
d)

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

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

Soportes físicos o electrónicos: Para la seguridad perimetral interior se cuenta con acceso a los espacios mediante puertas y cerraduras bajo llave. La administración de las llaves está a cargo de la Unidad Administrativa y cada usuario tiene su propia llave de acceso, cuando así sea el caso. Se cuenta con un sistema de tratamiento de datos personales mediante video vigilancia y control biométrico las 24 horas. Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Por ser trabajador de la DGELU, previamente registrado en el control de acceso biométrico bajo la autorización de la Unidad Administrativa de la DGELU.
2. ¿Cómo las autentifica?
   Mediante control biométrico.
3. ¿Cómo les autoriza el acceso?
   Mediante acceso automático.

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

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

Por el tipo de funcionamiento del sistema, no se requiere un procedimiento para la actualización de la información personal.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):
   a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
   No.
   b) ¿Es discrecional (matriz de control de acceso)?
   No.
   c) ¿Está basado en roles (perfiles) o grupos?
   No hay roles definidos.
   d) ¿Está basado en reglas?
   No hay reglas definidas.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
   a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
   No.
   b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
   No aplica.
   c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
   No aplica.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
   a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
   No aplica.

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No aplica.

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
No aplica.
b) ¿Quién autoriza la creación de nuevos perfiles?
No aplica.
c) ¿Se lleva registro de la creación de nuevos perfiles?
No aplica.

5. Acceso remoto al sistema de tratamiento de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No se requiere.
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
No.
c) ¿Cómo se evita el acceso remoto no autorizado?
No está configurado el acceso remoto.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos _Sí_, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual __x__,
   c) Periodicidad con que los realiza: _cada vez que hay modificaciones_
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad
   Se utiliza disco duro SSD o memoria USB.

[redacted] ver comentario [redacted]

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

IX. PLAN DE CONTINGENCIA

[redacted] ver comentario [redacted]

[redacted] ver comentario [redacted]

Eliminado: dos renglones con descripción correspondientes al Procedimiento de Respaldo y Recuperación de Datos y once renglones correspondientes al Plan de Contingencia. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
No aplica.

d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.
No aplica.

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria	
Identificador único*	SAP
(Nombre del sistema A3)*	Sistema Almacén de Publicaciones

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

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

Los datos personales se encuentran en una carpeta de argollas en el almacén, el acceso es mediante puerta con doble cerradura donde solo tiene llave el Jefe del Departamento de Publicaciones y el Director de Documentación y Difusión.

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

Nombre	Cargo	Funciones	Obligaciones
Jesús Antonio Sandoval Navarrete	Jefe del Departamento Publicaciones	Administrar la base datos de usuarios	Proteger los datos de los usuarios, almacenarlos en lugar seguro, realizar respaldos periódicamente, conservar la base, guardar en todo momento la confidencialidad del contenido de los datos.
Lic. Rafael González Zaldivar	Director de Documentación y Difusión	Gestionar la generación de los reportes que le soliciten las diferentes áreas internas de la DGELU, así como instancias universitarias. Recibir y dar trámite a las solicitudes de acceso al SAGICO. Notificar a los solicitan los nombres de usuario contraseñas de acceso	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la información de datos personales contenidos en los instrumentos consensuales. Proteger la integridad

		SAGICO.	SAGICO ante posib riesgos que alteren funcionalidad.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

a) **Los datos que se registran en las bitácoras:**
   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   b) Para soportes físicos: Número o clave del expediente utilizado, y
   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
b) Si las bitácoras están en soporte físico o en soporte electrónico;
c) Lugar dónde almacena las bitácoras y por cuánto tiempo;
d) La manera en que asegura la integridad de las bitácoras, y
e) Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

El Responsable del Sistema Almacén de Publicaciones es quien tiene el acceso a los datos personales, para el funcionamiento del propio almacén.

IV. REGISTRO DE INCIDENTES:

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

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) La metodología aplicada;
   c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
   d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

Para la pérdida o alteración no autorizada de expedientes en soportes físicos y electrónicos se levanta el acta administrativa correspondiente ante el titular de la DGELU, donde se consignen las situaciones de modo, tiempo y lugar y haga constar los hechos que se describen, para remitir a las instancias competentes.

V. ACCESO A LAS INSTALACIONES

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

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

Para el control de acceso a las instalaciones de la DGELU, se cuenta con dos puntos de acceso mediante control biométrico funcionando las 24 horas, operado por la Unidad Administrativa de la dependencia. También se cuenta con un sistema de video vigilancia las 24 horas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?
   Para personas que laboran en la DGELU, se identifican mediante el reconocimiento facial y/o la huella dactilar (control biométrico).
   Para personas ajenas a la dependencia, el personal interno atiende a las personas y pregunta e identifica el tipo de trámite que desean realizar en la DGELU, con base en las funciones, atribuciones y competencias de la dependencia.
b) ¿Cómo las autentifica?
   Para personas que laboran en la DGELU, mediante la comprobación de los elementos descritos en el inciso a) con los almacenados en la base de datos del control de acceso.
   Para personas ajenas a la dependencia, con la credencial de la UNAM, con credencial para votar con fotografía, con licencia de conducir u otra identificación que demuestre su identidad.
c) ¿Cómo les autoriza el acceso?
   Para personas que laboran en la DGELU, después de identificar y autenticar al personal, se permite el acceso automáticamente.
   Para personas ajenas a la dependencia: después de identificar y autenticar a la personal, se permite el acceso automáticamente.

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

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

Soportes físicos o electrónicos: Para la seguridad perimetral interior se cuenta con acceso a los espacios mediante puertas y cerraduras bajo llave. La administración de las llaves está a cargo de la Unidad Administrativa y cada usuario tiene su propia llave de acceso, cuando así sea el caso. Se cuenta con un sistema de tratamiento de datos personales mediante video vigilancia y control biométrico las 24 horas.

Para las personas que acceden a dichos espacios interiores:
1. ¿Cómo las identifica?
   Por ser trabajador de la DGELU, previamente registrado en el control de acceso biométrico bajo la autorización de la Unidad Administrativa de la DGELU.
2. ¿Cómo las autentifica?
   Mediante control biométrico.
3. ¿Cómo les autoriza el acceso?
   Mediante acceso automático.

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

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

Por el tipo de funcionamiento del sistema, no se requiere un procedimiento de actualización de información personal.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):
- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
  No.
- **b)** ¿Es discrecional (matriz de control de acceso)?
  No.
- **c)** ¿Está basado en roles (perfiles) o grupos?
  No hay roles definidos.
- **d)** ¿Está basado en reglas?
  No hay reglas definidas.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
  No.
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
  No aplica.
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  No aplica.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
  No aplica.
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
  No aplica.

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles?
  No aplica.

b) ¿Quién autoriza la creación de nuevos perfiles?
No aplica.

c) ¿Se lleva registro de la creación de nuevos perfiles?
No aplica.

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

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No se requiere.

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
No se requiere.

c) ¿Cómo se evita el acceso remoto no autorizado?
No está configurado el acceso remoto.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos _Sí_, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual __x__,
   c) Periodicidad con que los realiza: _cada vez que hay modificaciones_
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad[1]
   Se utiliza disco duro SSD o memoria USB.

[redacted] ver comentario [redacted]

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

IX. PLAN DE CONTINGENCIA

[redacted] ver comentario [redacted]

[redacted] ver comentario [redacted]

[redacted] ver comentario [redacted]

[1] Es deseable que precise si para almacenar dichos medios cuenta con al menos dos lugares distintos que cumplan con las condiciones de seguridad especificadas en el articulado del Capítulo V de los Lineamientos, conforme a la fracción III del Trigésimo primero de los Lineamientos; o bien, si utiliza un espacio externo seguro para guardar de manera sistemática dichos respaldos, según la fracción VIII del Trigésimo séptimo de tales Lineamientos.

Eliminado: dos renglones con descripción correspondientes al Procedimiento de Respaldo y Recuperación de Datos y catorce renglones correspondientes al Plan de Contingencia. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

No aplica.

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 Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)		
Identificador único*	SAGICO	
(Nombre del sistema A1)*	Sistema para la Administración y Gestión de Instrumentos Consensuales	
Recurso*	**Descripción***	**Control***
Revisión de cuentas de usuario activos.	Revisiones periódicas para determinar si tienen los permisos que deben de tener y cuales usuarios deben estar de baja.	Listado de usuarios activos. Responsable: Ing. Dulce María Milián García
Firewall actualizado	Revisar periódicamente el Firewall para verificar que se encuentre actualizado y no tenga alguna alerta de seguridad.	Licencia anual Responsable: Ing. Dulce María Milián García

Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General		
Identificador único*	Usuarios	
(Nombre del sistema A2)*	Biblioteca "Jorge Carpizo"	
Recurso*	**Descripción***	**Control***
Auditoría	Validar el debido cumplimiento de cada una de las actividades proyectadas en el plan de trabajo.	Mediante los responsables designados para el control y desarrollo de la verificación del debido cumplimiento.
Correo electrónico	Envío de los reportes generados mediante el correo electrónico	Los mensajes que contiene datos personales son cifrados y enviados directamente al usuario con privilegios administrativos.

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria	
Identificador único*	SAP

(Nombre del sistema A3)*	Sistema Almacén de Publicaciones	
Recurso*	**Descripción***	**Control***
Auditoría	Validar el debido cumplimiento de cada una de las actividades proyectadas en el plan de trabajo.	Mediante los responsables designados para el control y desarrollo de la verificación del debido cumplimiento.
Correo electrónico	Envío de los reportes generados mediante el correo electrónico	Los mensajes que contiene datos personales son cifrados y enviados directamente al usuario con privilegios administrativos.

7.2. Procedimiento para la revisión de las medidas de seguridad

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)		
Identificador único*	SAGICO	
(Nombre del sistema A1)*	Sistema para la Administración y Gestión de Instrumentos Consensuales	
Medida de seguridad*	**Procedimiento***	**Responsable***
Actualizar listado de usuarios activos	Comprobar que los usuarios del sistema tengan los privilegios adecuados para acceder solo a lo que les corresponde y comprobar que no se tenga usuarios activos que ya no laboren en DGELU.	Responsable: Ing. Dulce María Milián García Tiempo: 1 día
Actualizar el software antivirus y antimalware del Firewall	Comprobar que la protección software antivirus y antimalware del Firewall se encuentre actualizada.	Responsable: Ing. Dulce María Milián García Tiempo: 1 día
Respaldos periódicos de la aplicación y de la base de datos	Realizar respaldos de la base de datos, de la aplicación y de los documentos que contiene.	Responsable: Ing. Dulce María Milián García Tiempo: 1 día

Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General		
Identificador único*	Usuarios	
(Nombre del sistema A2)*	Biblioteca "Jorge Carpizo"	
Medida de seguridad*	**Procedimiento***	**Responsable***
Seguridad de los datos	Comprobar que el equipo	El Departamento de Cómputo.

personales de los usuarios resguardados en el equipo de cómputo del responsable de la biblioteca.	cuente con las actualizaciones correspondientes, en cuanto al software o hardware.	Un día.
Seguridad de los datos personales de los usuarios resguardados en carpeta física en la biblioteca	Comprobar que el espacio donde se resguardan los datos posee algún tipo de seguridad, como cerraduras bajo llave o acceso controlado.	a) La Unidad Administrativa. b) Un día.

ver comentario

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria		
Identificador único*	SAP	
(Nombre del sistema A3)*	Sistema Almacén de Publicaciones	
Medida de seguridad*	**Procedimiento***	**Responsable***
Seguridad de los datos personales de los usuarios resguardados en el equipo de cómputo del jefe del Departamento de Publicaciones.	Comprobar que el equipo cuente con las actualizaciones correspondientes, en cuanto al software o hardware.	El Departamento de Cómputo. Un día.
Seguridad de los datos personales de los usuarios resguardados en carpeta física en el Almacén de Publicaciones	Comprobar que el espacio donde se resguardan los datos posee algún tipo de seguridad, como cerraduras bajo llave o acceso controlado.	a) La Unidad Administrativa. b) Un día.

ver comentario

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

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)		
Identificador único*	SAGICO	
(Nombre del sistema A1)*	Sistema para la Administración y Gestión de Instrumentos Consensuales	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Actualizar listado de usuarios activos.	Los permisos de usuario se encuentran actualizados.	Responsable: Ing. Dulce María Milián García

Eliminado: seis recuadros con descripción correspondientes al Procedimiento para la revisión de las medidas de seguridad. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

Actualizar el software antivirus y antimalware del Firewall	El software se encuentra actualizado y se está gestionando la renovación de la licencia para que la protección continúe.	Responsable: Ing. Dulce María Milián García
Respaldos periódicos de la aplicación y de la base de datos	Se cuenta con respaldos diarios de la base de datos que se almacenan en una ubicación diferente al servidor. Respaldo mensual de todo el sitio.	Responsable: Ing. Dulce María Milián García

Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General		
Identificador único*	Usuarios	
(Nombre del sistema A2)*	Biblioteca "Jorge Carpizo"	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Actualizar base de datos de usuarios registrados.	La base de datos de usuarios registrados se encuentran actualizada.	Responsable: Ing. J. Antonio Sandoval Navarrete.
Respaldo de la de la base de datos.	Se cuenta con respaldos de la base de datos cada vez que hay una actualización de usuarios.	Responsable: Ing. J. Antonio Sandoval Navarrete.

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria		
Identificador único*	SAP	
(Nombre del sistema A3)*	Sistema Almacén de Publicaciones	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Actualizar base de datos de suscriptores registrados.	La base de datos de suscriptores se encuentra actualizada.	Responsable: Ing. J. Antonio Sandoval Navarrete.

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

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)	
Identificador único*	SAGICO

(Nombre del sistema A1)*	Sistema para la Administración y Gestión de Instrumentos Consensuales	
Medida de seguridad*	**Acciones***	**Responsable***
ver comentario		
ver comentario		
ver comentario		

Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General		
Identificador único*	Usuarios	
(Nombre del sistema A2)*	Biblioteca "Jorge Carpizo"	
Medida de seguridad*	**Acciones***	**Responsable***

En cuanto se tengan los resultados de la evaluación, se aplicarán las acciones para la corrección y actualización de las medidas de seguridad.

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria		
Identificador único*	SAP	
(Nombre del sistema A3)*	Sistema Almacén de Publicaciones	
Medida de seguridad*	**Acciones***	**Responsable***
ver comentario		

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Eliminado: doce recuadros con descripción correspondientes a las Acciones para la corrección y actualización de las medidas de seguridad. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)	
Identificador único*	SAGICO
(Nombre del sistema A1)*	Sistema para la Administración y Gestión de Instrumentos Consensuales
Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General	
Identificador único*	Usuarios
(Nombre del sistema A2)*	Biblioteca "Jorge Carpizo"
Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria	
Identificador único*	SAP
(Nombre del sistema A3)*	Sistema Almacén de Publicaciones

Actividad*	Descripción*	Duración*	Cobertura*
Programa de capacitación sobre protección de datos personales	Curso en línea	22 al 25 de marzo del 2022, 9:00 a 11:30 hrs.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin frecuencia de actualización.
Elaboración de Documento de Seguridad y del Sistema de Gestión de Seguridad de Datos Personales	Curso en línea	22 al 25 de marzo del 2022, 12:00 a 14:30 hrs.	Público objetivo: Enlaces de Transparencia, Responsables de Seguridad de Datos Personales, Responsables de Tecnologías de la Información, así como funcionarios y empleados universitarios. Sin vigencia. Sin vigencia. Sin frecuencia de actualización.

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

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)

Identificador único*	SAGICO
(Nombre del sistema A1)*	Sistema para la Administración y Gestión de Instrumentos Consensuales
Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General	
Identificador único*	Usuarios
(Nombre del sistema A2)*	Biblioteca "Jorge Carpizo"
Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria	
Identificador único*	SAP
(Nombre del sistema A3)*	Sistema Almacén de Publicaciones

Como medidas de difusión de la protección de datos personales, se cuenta con avisos de privacidad (integrales y simplificados) de la Biblioteca y de la DGELU en los que se hace del conocimiento a los interesados que el tratamiento de sus datos personales forma parte de las medidas de seguridad adoptadas al interior de dichas instalaciones, a través de los sistemas de control de acceso biométrico y circuito cerrado de televisión, así como el ejercicio de derechos Acceso, Rectificación, Cancelación y Oposición (ARCO).

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)			
Identificador único*	SAGICO		
(Nombre del sistema A1)*	Sistema para la Administración y Gestión de Instrumentos Consensuales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
ver comentario			
ver comentario			

Eliminado: ocho recuadros con descripción correspondientes a la Mejora Continua. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

	ver comentario		ver comentario

Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General	
Identificador único*	Usuarios
(Nombre del sistema A2)*	Biblioteca "Jorge Carpizo"

No se tiene planeado, a corto plazo, ningún proyecto de actualización.

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria	
Identificador único*	SAP
(Nombre del sistema A3)*	Sistema Almacén de Publicaciones

El sistema se actualizó en 2021 y por el momento no se considera modificarlo.

9.2. Actualización y mantenimiento de equipo de cómputo

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)			
Identificador único*	SAGICO		
(Nombre del sistema A1)*	Sistema para la Administración y Gestión de Instrumentos Consensuales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento preventivo	Llevar a cabo actividades encaminadas a mantener funcionales los equipos de cómputo de la DGELU	Un mes.	Se reduce al mínimo el riesgo de pérdida de datos por falla del equipo
Actualización de equipo	Llevar a cabo acciones para incrementar la	Las actualizaciones dependerán de los recursos asignados	Se reduce al mínimo el riesgo de pérdida de datos por falla del equipo

Eliminado: dos recuadros con descripción correspondientes a las Mejoras Continuas. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

	capacidad de procesamiento y almacenamiento del equipo.	y, en su caso, se efectúan a equipos considerados críticos. Dos días.	

Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General	
Identificador único*	Usuarios
(Nombre del sistema A2)*	Biblioteca "Jorge Carpizo"

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria	
Identificador único*	SAP
(Nombre del sistema A3)*	Sistema Almacén de Publicaciones

Conforme a lo dispuesto en el Programa de Racionalidad Presupuestal 2022 de la UNAM, no se tiene considerado realizar acciones de actualización y mantenimiento al equipo de cómputo para la Biblioteca y el Almacén de Publicaciones.

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

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)		
Identificador único*	SAGICO	
(Nombre del sistema A1)*	Sistema para la Administración y Gestión de Instrumentos Consensuales	
Proceso*	**Descripción***	**Responsable***
Respaldo de la base de datos del sistema.	El respaldo se lleva a cabo diariamente y se almacena en un medio diferente al servidor para su conservación en caso de alguna eventualidad.	Responsables: Ing. Dulce María Milián García. Ing. David Ricardo Montalván Rodriguez.
Respaldo del Sistema	El respaldo del sistema y los documentos que contiene se lleva a cabo de manera mensual y se almacena en un medio diferente al servidor.	Responsable: Ing. Dulce María Milián García
Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General		

Identificador único*	Usuarios
(Nombre del sistema A2)*	Biblioteca "Jorge Carpizo"

Se cuenta con procesos manuales para la conservación, preservación y respaldos de información.

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria	
Identificador único*	SAP
(Nombre del sistema A3)*	Sistema Almacén de Publicaciones

Se cuenta con procesos manuales para la conservación, preservación y respaldos de información.

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

Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)		
Identificador único*	SAGICO	
(Nombre del sistema A1)*	Sistema para la Administración y Gestión de Instrumentos Consensuales	
Disposición final de equipos o componentes de cómputo.	1. El Departamento de Cómputo genera el listado de los equipos destinados a la baja. 2. La Unidad Administrativa de la DGELU verifica los equipos inventariables y de control interno. 3. Se recibe la autorización de la Unidad Administrativa. 4. Se solicita a la Dirección General de Patrimonio la baja y se programa una visita por para verificar el estado físico de los equipos. 5. Una vez verificado el punto anterior, se acepta la baja por desuso y se programa una fecha para la entrega física en el Área de Bajas de la Dirección General de Patrimonio. 6. Se realiza la entrega física de los equipos con documentos de entrega-recepción.	Unidad Administrativa.

	7. Se concluye el proceso eliminando los equipos del Sistema de Control Patrimonial (SICOP).	

Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General		
Identificador único*	Usuarios	
(Nombre del sistema A2)*	Biblioteca "Jorge Carpizo"	
Disposición final de equipos o componentes de cómputo.	1. El Departamento de Cómputo genera el listado de los equipos destinados a la baja. 2. La Unidad Administrativa de la DGELU verifica los equipos inventariables y de control interno. 3. Se recibe la autorización de la Unidad Administrativa. 4. Se solicita a la Dirección General de Patrimonio la baja y se programa una visita por para verificar el estado físico de los equipos. 5. Una vez verificado el punto anterior, se acepta la baja por desuso y se programa una fecha para la entrega física en el Área de Bajas de la Dirección General de Patrimonio. 6. Se realiza la entrega física de los equipos con documentos de entrega-recepción. 7. Se concluye el proceso eliminando los equipos del Sistema de Control Patrimonial (SICOP).	Unidad Administrativa.

Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria		
Identificador único*	SAP	
(Nombre del sistema A3)*	Sistema Almacén de Publicaciones	
Proceso*	**Descripción***	**Responsable***
Disposición final de equipos	1. El Departamento de	Unidad Administrativa.

o componentes de cómputo.	Cómputo genera el listado de los equipos destinados a la baja. 2. La Unidad Administrativa de la DGELU verifica los equipos inventariables y de control interno. 3. Se recibe la autorización de la Unidad Administrativa. 4. Se solicita a la Dirección General de Patrimonio la baja y se programa una visita por para verificar el estado físico de los equipos. 5. Una vez verificado el punto anterior, se acepta la baja por desuso y se programa una fecha para la entrega física en el Área de Bajas de la Dirección General de Patrimonio. 6. Se realiza la entrega física de los equipos con documentos de entrega-recepción. 7. Se concluye el proceso eliminando los equipos del Sistema de Control Patrimonial (SICOP).	

ver comentario

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

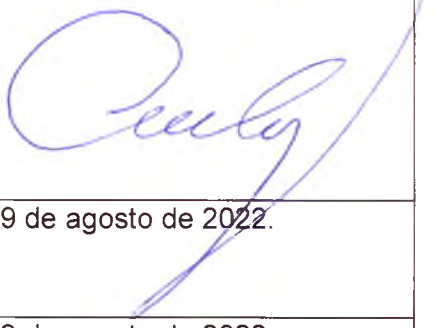
11. Departamento de Cómputo de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)	
Identificador único*	SAGICO
(Nombre del sistema A1)*	Sistema para la Administración y Gestión de Instrumentos Consensuales
Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General	
Identificador único*	Usuarios
(Nombre del sistema A2)*	Biblioteca "Jorge Carpizo"
Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria	

Eliminado: dos renglones con descripción correspondientes a los Procesos de Borrados Seguro. Fundamento Legal: Arts. 113, fracción VII de la LGTAIP y 110, fracción VII de la LFTAIP. En virtud de tratarse de información cuya publicación obstruye la prevención de los delitos. Reservado por 5 años.

Identificador único*	SAP
(Nombre del sistema A3)*	Sistema Almacén de Publicaciones

Debido a las funciones e importancia de cada sistema, se considera no necesario tener un procedimiento de cancelación de sistemas de tratamiento de datos personales.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Ing. Dulce María Milián García, Jefa de Departamento de Cómputo y Automatización, tel. (55) 5622-6377 Ext. 48077, dulcemilian@comunidad.unam.mx Ing. J. Antonio Sandoval Navarrete, Jefe del Departamento de Publicaciones, tel. (55) 5622-6377 Ext. 48047, jasan@unam.mx	
Revisó:	Lic. Rafael González Zaldivar, Director de Documentación y Difusión, tel. (55) 5622-6377 Ext. 48071, ragonzal@unam.mx	
Autorizó:	Dr. Daniel Márquez Gómez, Director General de Estudios de Legislación Universitaria, tel. (55) 5622-6377 Ext. 48085, dgelu@unam.mx	
Fecha de aprobación:	(Incluir la fecha de liberación del documento)	19 de agosto de 2022.
Fecha de actualización:	(Incluir la primer versión e ir agregando las subsiguientes del documento)	19 de agosto de 2022.

Dirección General de Estudios de Legislación Universitaria
Documento de seguridad
Partes clasificadas: dos renglones en donde se especifican las características del lugar donde se resguardan los soportes, pág. 20 y un reglón, relacionado con la descripción de soporte, págs. 20 y 21; doce cuadros con descripción correspondientes al Análisis de Riesgo, pág. 21; veinticinco cuadros con descripción correspondientes al Análisis de Riesgo, pág. 22; veintinueve cuadros con descripción correspondientes al Análisis de Riesgo, pág. 23; seis cuadros con descripción correspondientes al Análisis de Riesgo y seis cuadros con descripción correspondientes al Análisis de Brecha, pág. 24; doce cuadros con descripción correspondientes al Análisis de Riesgo y seis renglones correspondientes al Plan de Trabajo, pág.25; dieciséis cuadros con descripción correspondientes al Plan de Trabajo, pág. 26; veintiún cuadros con descripción correspondientes al Plan de Trabajo, pág. 27; cuatro cuadros con descripción correspondientes al Plan de Trabajo, pág. 28; once renglones con descripción correspondientes al Resguardo de Sistemas de Tratamiento de Datos Personales con Soportes Físicos, pág. 30; un renglón con descripción correspondientes a las Bitácoras para Acceso y Operación Cotidiana, pág. 31; once renglones con descripción al perfil de usuario y contraseñas, pág. 33; dos renglones con descripción correspondientes al Procedimientos de Respaldo y Recuperación de Datos, págs. 34, 38, 43; dieciséis renglones correspondientes al Plan de Contingencia y dos renglones correspondientes al Resguardo de Sistemas de Tratamiento de Datos Personales con Soporte Físico, pág. 34; once renglones correspondientes al Plan de Contingencia,pág. 38; catorce renglones correspondientes al Plan de Contingencia, pág. 43; seis recuadros con descripción correspondientes a los Procedimientos para la revisión de las medidas seguridad, pág. 46; doce recuadros con descripción correspondientes a las Acciones para la corrección y actualización de las medidas de seguridad. 48; ocho recuadros con descripción correspondientes a las Mejoras Continuas, pág. 50; dos recuadros con descripción correspondientes a las Mejoras Continuas, 51 y dos renglones con descripción correspondientes a los Procesos de Borrados Seguro, pág. 55.
Fundamento Legal: Arts. 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracciones VII de la Ley Federal de Transparencia y Acceso a la Información Pública. En virtud de tratarse de información que cobstruye la prevención de los delitos.
Reservado por 5 años.
Fecha y número de acta de la sesión: 19/08/2022 y CTUNAM/525/2022.
MIMC.

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/525/2022

Visto el expediente relativo a la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública , que someten el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** en relación con sus respectivos **Documentos de Seguridad**, se procede a dictar la presente resolución con base en los siguientes:

A N T E C E D E N T E S

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 permitirán 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 resulten 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 artículos 247 y 248 de 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.

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 Púbica 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. La Presidencia del Comité de Transparencia recibió diversos oficios, mediante los cuales las Áreas Universitarias sometieron a consideración de este Cuerpo Colegiado, la clasificación parcial de información reservada de sus Documentos de Seguridad, mismos que se enlistan a continuación:

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/525/2022

Oficio	Área Universitaria	Fecha de presentación
IMAT/D048/2022	Instituto de Matemáticas	15/08/2022
IFCE/DIR/184/2022	Instituto de Fisiología Celular	
CCHDG/DIR/145/08/2022	Dirección General de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHA/DIR/415/VIII/2022	Plantel Azcapotzalco de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHN.91.20/580/2022	Plantel Naucalpan de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHO/DIR/445/2022	Plantel Oriente de la Escuela Nacional Colegio de Ciencias y Humanidades	
OF/CCHS/DIR/160/2022	Plantel Sur de la Escuela Nacional Colegio de Ciencias y Humanidades	
CCHV/OJ/135/2022	Plantel Vallejo de la Escuela Nacional Colegio de Ciencias y Humanidades	
FFLE/CP/034/2022	Facultad de Filosofía y Letras	
CODC/182/2022	Coordinación de Difusión Cultural	
DGEL/JT/3454/2022	Dirección General de Estudios de Legislación Universitaria	16/08/2022
CUTE/DIR/66/2022	Centro Universitario de Teatro	
DGRU/115/2022	Dirección General de Radio UNAM	
SDI/116/2022	Secretaría de Desarrollo Institucional	17/08/2022
IFIS/D/221/2022 IFIS/D/223/2022	Instituto de Física	
CJBS/112/22	Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud	
CAI/063/2022	Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías	
DIR/MUCH/0160/2022	Museo Universitario del Chopo	
DGMU/114/08/2022	Dirección General de Música	
DDAN/0356/2022	Dirección de Danza	
CIGA/D/133/2022	Centro de Investigaciones en Geografía Ambiental, Campus Morelia	
DiGAV/D/2315/2022	Museo Universitario de Arte Contemporáneo	
DDUIAVG/T/2427/2022	Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género	
IQUI 427/2022	Instituto de Química	
DLFL/208/2022	Dirección de Literatura y Fomento a la	

	Lectura	
DGSA/0381/2022	Dirección General de Servicios Administrativos	
DTEA/107/2022	Dirección de Teatro UNAM	
ENP3/DIRE/239/2022	Escuela Nacional Preparatoria, Plantel 3	
CCG/DIR/293/2022	Centro de Ciencias Genómicas	
FAD/DIR/445/2022	Facultad de Artes y Diseño	
DGTV/DG/197/2022	Dirección General de Televisión Universitaria	
CCUT/139/2022	Centro Cultural Universitario Tlatelolco	
ENPDG/314/2022	Dirección General de la Escuela Nacional Preparatoria	
DGOAE/416/2022	Dirección General de Orientación y Atención Educativa	
CJCS/124/2022	Consejo Académico del Área de las Ciencias Sociales	
ENES/MID/OFJ/199/2022	Escuela Nacional de Estudios Superiores, Unidad Mérida	
IECO/DIR/327/2022	Instituto de Ecología	
DGECI/DG/0869/2022	Dirección General de Cooperación e Internacionalización	
IIB/DIR/309/2022	Instituto de Investigaciones Biomédicas	
DCLA/Of.096/2022	Casa del Lago "Mtro Juan José Arreola"	
ENP4/DIR/108/2022	Escuela Nacional Preparatoria, Plantel 4	
CIG/C/320/2022	Coordinación para la Igualdad de Género	
DGDU/CJ/930/2022	Dirección General del Deporte Universitario	

En dichos oficios, las Áreas Universitarias informaron 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 Obligados[1]; 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*

[1] *DOF: 26 de noviembre de 2021*

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 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 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 … 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	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica … y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	…
b) Análisis de brecha	*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.*	…
c) Plan de Trabajo	*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.*	…

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, las políticas de respaldo 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.*

- *Divulgar el análisis de riesgo, el análisis de brecha … y el plan de trabajo … 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, las políticas de respaldo 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.

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 32 y 36 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:

C O N S I D E R A C I O N E S

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, entre otras Áreas Universitarias, por la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género**, así como por la **Dirección General de Estudios de Legislación Universitaria**, dependiente de la Oficina de la Abogacía General, en este acto, la Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género e integrante de este Cuerpo Colegiado, Guadalupe Barrena Nájera, el Abogado General y Presidente del Comité de Transparencia, Alfredo Sánchez Castañeda, así como el Director General de Asuntos Jurídicos y

Secretario Técnico de este Comité, Lic. Jorge Barrera Gutiérrez, formalmente se excusan de conocer del caso, para no afectar la imparcialidad del mismo.

SEGUNDA. De conformidad con lo dispuesto en los artículos 1, 10 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 de los Documentos de Seguridad, propuesta por el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** y determinar, en consecuencia, si la confirma, modifica o revoca.

TERCERA. De conformidad con lo dispuesto en los artículos 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, el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de**

Física, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** clasificaron como información reservada, por un periodo de **cinco años**, la relativa al **Análisis de Riesgo**, al **Análisis de Brecha** y al **Plan de Trabajo**, 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.

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 para evitar la comisión de los mismos, o bien, por menoscabar o limitar la 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.

Desde el punto de vista criminológico, prevenir es 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 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 podrá 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, 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 ese sentido, 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 administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales del Área Universitaria, 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.

En este sentido, 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 de las Áreas Universitarias,** 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 ocasionar la pérdida, 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 **Plan de Trabajo**, así como **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 de las Áreas Universitarias**, tiene como propósito evitar o prevenir la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema 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 de las Áreas Universitarias**, por lo que la misma protección deberá otorgarse a los sistemas electrónicos, así como a los archivos físicos con los que se cuenta.

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 de las Áreas Universitarias,** la cual se encuentra contenida en los documentos de seguridad remitidos por las Áreas Universitarias, se darían a conocer las acciones implementadas o por implementar, de acuerdo con el análisis de riesgos y de brecha, priorizando 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 del responsable, manejo de documentos físicos y/o electrónicos, entre otros, lo que representa para las Áreas Universitarias un riesgo evidente para la estabilidad de la ejecución de las medidas de seguridad adoptadas para resguardar los datos en su poder, en tanto la publicación de esa información revelaría 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 de las Áreas Universitarias, 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 de las Áreas Universitarias, 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 solicitada 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.

De difundirse el plan de trabajo, el análisis de riesgos y el análisis de brecha del documento de seguridad, se afectarían las medidas y acciones implementadas por las Áreas Universitarias para reducir el riesgo de que se cometa una conducta o un comportamiento que pueda dañar o convertir a esta Universidad y su comunidad en sujetos o víctimas de conductas ilícitas.

Lo anterior, toda vez que la publicidad de la información contenida en el **análisis de riesgos, de brecha** y el **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 de las Áreas Universitarias**, representa un riesgo potencial para las Áreas Universitarias, 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 de las Áreas Universitarias 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 al interés público la divulgación de la información en cuestión, supera al perjuicio que se ocasionaría al no publicarla, pues con la difusión de la información contenida en el **análisis de riesgos, de brecha y el 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 de las Áreas Universitarias**, se limitaría la capacidad de las Áreas Universitarias 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.

Se considera que la limitación de acceso a la información solicitada se ajusta al principio de proporcionalidad, toda vez que se justifica negar su acceso, a cambio de garantizar la capacidad de las Áreas Universitarias 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 las Áreas Universitarias, en el desempeño y/o ejercicio de sus competencias, facultades o funciones.

En ese sentido, 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 se computará a partir de la fecha en que se emite la presente resolución y hasta la fecha de término del periodo, o bien, se interrumpirá antes si desaparecen las causas que originaron la reserva de la información, lo que suceda primero. 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, en su momento, ya que éste no se verá restringido por un periodo mayor al previsto por la norma.

Por lo antes mencionado, se colman las hipótesis de las fracciones I, II y III, dispuestas en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, por lo que es procedente **CONFIRMAR** la reserva total de una parte de la información para la elaboración de la

versión pública propuesta por el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la Escuela Nacional Preparatoria** y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** por un periodo de **cinco años**, que se computarán 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. Este Comité considera pertinente orientar a las Áreas Universitarias, a efecto de que en la elaboración de la versión pública de sus respectivos documentos de seguridad, tengan en cuenta lo siguiente:

- Deberán 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 deberán emplear 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.

- Deberán 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.

Lo anterior, de conformidad con lo dispuesto en los numerales 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, 113, fracción VII, 137 inciso a) de la Ley General de Transparencia y Acceso a la Información Pública; 65, 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, 38, último párrafo del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, este Comité de Transparencia:

R E S U E L V E

PRIMERO. Con fundamento en lo dispuesto en los artículos 1, 10, 11, 15 fracción X y 31, fracción I 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** total de una parte la información para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por el **Instituto de Matemáticas,** el **Instituto de Fisiología Celular,** la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, la **Facultad de Filosofía y Letras,** la **Coordinación de Difusión Cultural**, la **Dirección General de Estudios de Legislación Universitaria,** el **Centro Universitario de Teatro,** la **Dirección General de Radio UNAM,** la **Secretaría de Desarrollo Institucional,** el **Instituto de Física**, el **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** el **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** el **Museo Universitario del Chopo,** la **Dirección General de Música,** la **Dirección de Danza,** el **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** el **Museo Universitario de Arte Contemporáneo,** la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** el **Instituto de Química,** la **Dirección de Literatura y Fomento a la Lectura,** la **Dirección General de Servicios Administrativos,** la **Dirección de Teatro UNAM,** el **Centro de Ciencias Genómicas,** la **Facultad de Artes y Diseño,** la **Dirección General de Televisión Universitaria,** el **Centro Cultural Universitario Tlatelolco,** la **Dirección General de Orientación y Atención Educativa,** el **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** el **Instituto de Ecología,** la **Dirección General de Cooperación e Internacionalización,** el **Instituto de Investigaciones Biomédicas,** la **Casa del Lago "Mtro. Juan José Arreola",** la **Coordinación para la Igualdad de Género,** la **Dirección General de la**

Escuela Nacional Preparatoria y la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera"** y la **Dirección General del Deporte Universitario,** en relación con el **Análisis de Riesgos**, el **Análisis de Brecha** y el **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 de las Áreas Universitarias**, por un periodo de **cinco años**, contados a partir de la fecha de la presente resolución, o bien, hasta en tanto se extingan las causas que dieron origen a la reserva de la información.

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

SEGUNDO. Se instruye a las Áreas Universitarias a efecto de que elaboren la versión pública en términos de lo dispuesto en la consideración **CUARTA.**

TERCERO. 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 53, fracción VI, inciso c) del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, notifíquese la presente resolución por correo institucional al **Instituto de Matemáticas,** al **Instituto de Fisiología Celular,** a la **Dirección General de la Escuela Nacional Colegio de Ciencias** y **Humanidades,** a la **Escuela Nacional Colegio de Ciencias y Humanidades Planteles Azcapotzalco, Vallejo, Naucalpan, Oriente y Sur**, a la **Facultad de Filosofía y Letras,** a la **Coordinación de Difusión Cultural**, a la **Dirección General de Estudios de Legislación Universitaria,** al **Centro Universitario de Teatro,** a la **Dirección General de Radio UNAM**, a la **Secretaría de Desarrollo Institucional,** al **Instituto de Física**, al **Consejo Académico del Área de las Ciencias Biológicas, Químicas y de la Salud,** al **Comité de Análisis para las Intervenciones Urbanas, Arquitectónicas y de las Ingenierías,** al **Museo Universitario del Chopo,** a la **Dirección General de Música,** a la **Dirección de Danza,** al **Centro de Investigaciones en Geografía Ambiental, Campus Morelia,** al **Museo Universitario de Arte Contemporáneo,** a la **Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género,** al **Instituto de Química,** a la **Dirección de Literatura y Fomento a la Lectura,** a la **Dirección General de Servicios Administrativos,** a la **Dirección de Teatro UNAM,** al **Centro de Ciencias Genómicas,** a la **Facultad de Artes y Diseño,** a la **Dirección General de Televisión Universitaria,** al **Centro Cultural Universitario Tlatelolco,** a la **Dirección General de Orientación y Atención Educativa,** al **Consejo Académico del Área de las Ciencias Sociales,** la **Escuela Nacional de Estudios Superiores, Unidad Mérida,** al **Instituto de Ecología,** a la **Dirección General de Cooperación e Internacionalización,** al **Instituto de Investigaciones Biomédicas,** a la **Casa del Lago "Mtro. Juan José Arreola",** a la **Coordinación para la Igualdad de Género,** a la **Dirección General de la Escuela Nacional Preparatoria** y a la **Escuela Nacional Preparatoria, Planteles 3 "Justo Sierra"** y **4 "Vidal Castañeda y Nájera",** a la **Dirección General del Deporte Universitario,** así como a la Unidad de Transparencia de esta Universidad, para los efectos procedentes.

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, 20 y 53,

fracción VI 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., 19 de agosto de 2022

Archivo	08-ctunam-525-2022-docto-seg-1.pdf		
Identificador único (hash)	5c7a552404c38ce4b052cc8e212d4579a13448672db8ce248b096c2e568ad6cf		
Fecha y hora de cierre	19/08/2022 16:28:33	**Fecha y hora de emisión**	19/08/2022 16:30:53
Número de páginas	19	**Firmantes**	4

Firmantes

Nombre	Lic. MARIA ELENA GARCIA MELENDEZ	**Fecha y hora de firma**	19/08/2022 15:18:41
Directora General para la Prevención y Mejora de la Gestión Institucional y Suplente del Contralor			
Hash Firma	cbaca6eb689a47d8770065a6f6ff297b80269e390ef3f832d480a433bf1abbfbf4ed2ced4f3f344361b247c806f9e1e2		

Nombre	Ing. Ricardo Ramírez Ortiz	**Fecha y hora de firma**	19/08/2022 15:41:03
Director General de Servicios Generales y Movilidad			
Hash Firma	1ad0c05aa515c5cfb0a9def95dd4b62ff2c74d8447fbdc4130479cece21b04b4035d4865b90866689b75f86c70c2ce60		

Nombre	JOSE MELJEM MOCTEZUMA	**Fecha y hora de firma**	19/08/2022 16:28:33
Titular de la Unidad de Transparencia			
Hash Firma	8d01b7ff1fe5c4c30fcea6d96019f992ef58adde4f23ce469572c785c60d3e1d5d9bbef4bfee618dddfc45f27edac3db		

Nombre	Dra. Jacqueline Peschard Mariscal	**Fecha y hora de firma**	19/08/2022 16:19:26
Especialista			
Hash Firma	460b366695dd8e79de4878edcf8017579ce607f70964c5cabc1bcba1cdfd08f60261a88559c3ef1d8ea03ae660538626		