



# Documento de Seguridad de Datos Personales

**Dirección General de Estudios de  
Legislación Universitaria**

Enero 2024



# DGELU

DIRECCIÓN GENERAL DE ESTUDIOS  
DE LEGISLACIÓN UNIVERSITARIA



**DIRECCIÓN GENERAL DE ESTUDIOS DE LEGISLACIÓN  
UNIVERSITARIA**

**DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES**

## ÍNDICE

Introducción

Objetivos

Definiciones

1. Inventario de sistemas de tratamiento de datos personales
2. Estructura y descripción de los sistemas de tratamiento de datos personales
3. Análisis de riesgos
4. Análisis de brecha
5. Plan de trabajo
6. Medidas de seguridad implementadas
7. Mecanismos de monitoreo y revisión de las medidas de seguridad
8. Programa específico de capacitación
9. Mejora continua
10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales
11. Aprobación del documento de seguridad

## 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, filmicos, 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

<b>Departamento de Cómputo y Automatización de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)</b>	
<b>Identificador único*</b>	SAGICO
<b>(Nombre del sistema A1) *</b>	Sistema para la Administración y Gestión de Instrumentos Consensuales
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	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.
<b>Responsable*:</b>	
<b>Nombre*:</b>	<b>Mtro. Hans Kohler Lizardi</b>
<b>Cargo*:</b>	<b>Jefe del Departamento de Cómputo y Automatización de la DGELU</b>
<b>Funciones*:</b>	Recibir y dar trámite a las solicitudes de acceso al SAGICO. Generar los nombres de usuario y contraseñas para el acceso al SAGICO. Consultar la información y generar los reportes que le soliciten las instancias universitarias y las áreas internas de la DGELU. 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.
<b>Obligaciones*:</b>	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 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.



<b>Encargados:</b>	
<b>(Nombre del Encargado 1*)</b>	<b>Lic. Rafael González Zaldivar</b>
<b>Cargo*:</b>	<b>Director de Documentación y Difusión</b>
<b>Funciones*:</b>	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.
<b>Obligaciones*:</b>	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.
<b>(Nombre del Encargado 2*)</b>	<b>Ing. David Ricardo Montalván Rodríguez</b>
<b>Cargo*:</b>	<b>Asistente de Procesos</b>
<b>Funciones*:</b>	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.
<b>Obligaciones*:</b>	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.
<b>Usuarios:</b>	
<b>Dirección General</b>	
<b>(Nombre del Usuario 1*)</b>	<b>Dra. Ángela Quiroga Quiroga</b>
<b>Cargo*:</b>	<b>Directora General de Estudios de Legislación Universitaria</b>

<b>Funciones*:</b>	Consultar los instrumentos consensuales almacenados en el SAGICO.
<b>Obligaciones*:</b>	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.
<b>(Nombre del Usuario 2*)</b>	<b>Lic. José Abraham González Becerra</b>
<b>Cargo*:</b>	<b>Coordinador de Gestión</b>
<b>Funciones*:</b>	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.
<b>Obligaciones*:</b>	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.
<b>Dirección de Convenios</b>	
<b>(Nombre del Usuario 1*)</b>	<b>Cristina Galicia Vázquez</b>
<b>Cargo*:</b>	<b>Encargada de despacho</b>
<b>Funciones*:</b>	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.
<b>Obligaciones*:</b>	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.
<b>(Nombre del Usuario 2*)</b>	<b>Karla Gabriela Hernández Andrade</b>
<b>Cargo*:</b>	<b>Jefa del Departamento de Instrumentos Consensuales Nacionales</b>
<b>Funciones*:</b>	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.
<b>Obligaciones*:</b>	Proteger los datos personales de los involucrados en los instrumentos consensuales.

	<p>No modificar los datos personales contenidos en los instrumentos consensuales.</p> <p>No difundir la información de datos personales contenidos en los instrumentos consensuales.</p> <p>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.</p>
<b>(Nombre del Usuario 3*)</b>	<b>Cristina Galicia Vázquez</b>
<b>Cargo*:</b>	<b>Jefa del Departamento de Instrumentos Consensuales Internacionales</b>
<b>Funciones*:</b>	<p>Realizar el seguimiento, consulta de antecedentes y control de los instrumentos consensuales asignados al área de Convenios.</p> <p>Consultar, analizar y generar reportes de los instrumentos consensuales almacenados en el SAGICO.</p>
<b>Obligaciones*:</b>	<p>Proteger los datos personales de los involucrados en los instrumentos consensuales.</p> <p>No modificar los datos personales contenidos en los instrumentos consensuales.</p> <p>No difundir la información de datos personales contenidos en los instrumentos consensuales.</p> <p>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.</p>
<b>(Nombre del Usuario 4*)</b>	<b>Erika Alejandra Suárez Guevara</b>
<b>Cargo*:</b>	<b>Secretaria Auxiliar</b>
<b>Funciones*:</b>	<p>Consultar, capturar, turnar, dar seguimiento, realizar análisis y editar la información de identificación de los instrumentos consensuales alojados en el SAGICO.</p> <p>Administrar los datos de las “contrapartes” señaladas en los instrumentos consensuales.</p> <p>Intercambiar y verificar información con la Dirección de Apoyo Normativo a Comités y Contratos.</p>
<b>Obligaciones*:</b>	<p>Proteger los datos personales de los involucrados en los instrumentos consensuales.</p> <p>No modificar los datos personales contenidos en los instrumentos consensuales.</p> <p>No difundir la información de datos personales contenidos en los instrumentos consensuales.</p> <p>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.</p>
<b>(Nombre del Usuario 5*)</b>	<b>Daniel Alejandro Ramírez García</b>
<b>Cargo*:</b>	<b>Abogado Auxiliar</b>
<b>Funciones*:</b>	<p>Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.</p>

<b>Obligaciones*:</b>	<p>Proteger los datos personales de los involucrados en los instrumentos consensuales.</p> <p>No modificar los datos personales contenidos en los instrumentos consensuales.</p> <p>No difundir la información de datos personales contenidos en los instrumentos consensuales.</p> <p>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.</p>
<b>(Nombre del Usuario 6*)</b>	<b>Luis Daniel Luna Santacruz</b>
<b>Cargo*:</b>	<b>Abogado Auxiliar</b>
<b>Funciones*:</b>	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
<b>Obligaciones*:</b>	<p>Proteger los datos personales de los involucrados en los instrumentos consensuales.</p> <p>No modificar los datos personales contenidos en los instrumentos consensuales.</p> <p>No difundir la información de datos personales contenidos en los instrumentos consensuales.</p> <p>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.</p>
<b>(Nombre del Usuario 7*)</b>	<b>Kevin Granados Flores</b>
<b>Cargo*:</b>	<b>Abogado Auxiliar</b>
<b>Funciones*:</b>	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
<b>Obligaciones*:</b>	<p>Proteger los datos personales de los involucrados en los instrumentos consensuales.</p> <p>No modificar los datos personales contenidos en los instrumentos consensuales.</p> <p>No difundir la información de datos personales contenidos en los instrumentos consensuales.</p> <p>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.</p>
<b>(Nombre del Usuario 8*)</b>	<b>Marco Antonio Núñez Campuzano</b>
<b>Cargo*:</b>	<b>Abogado Auxiliar</b>
<b>Funciones*:</b>	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
<b>Obligaciones*:</b>	<p>Proteger los datos personales de los involucrados en los instrumentos consensuales.</p> <p>No modificar los datos personales contenidos en los instrumentos consensuales.</p> <p>No difundir la información de datos personales contenidos</p>

	<p>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.</p>
<b>(Nombre del Usuario 9*)</b>	<b>Eleazar Albarrán Vergara</b>
<b>Cargo*:</b>	<b>Abogado Auxiliar</b>
<b>Funciones*:</b>	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
<b>Obligaciones*:</b>	<p>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.</p>
<b>(Nombre del Usuario 10*)</b>	<b>Emmanuel Coraza Pérez</b>
<b>Cargo*:</b>	<b>Abogado Auxiliar</b>
<b>Funciones*:</b>	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
<b>Obligaciones*:</b>	<p>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.</p>
<b>(Nombre del Usuario 11*)</b>	<b>María Alejandra Sánchez Vite</b>
<b>Cargo*:</b>	<b>Abogada Auxiliar</b>
<b>Funciones*:</b>	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
<b>Obligaciones*:</b>	<p>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.</p>

<b>(Nombre del Usuario 12*)</b>	<b>Soledad Iliana Orihuela Aguilar</b>
<b>Cargo*:</b>	<b>Abogada Auxiliar</b>
<b>Funciones*:</b>	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
<b>Obligaciones*:</b>	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.
<b>(Nombre del Usuario 13*)</b>	<b>Lizbet Guadalupe Flores Gómez</b>
<b>Cargo*:</b>	<b>Abogada Auxiliar</b>
<b>Funciones*:</b>	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.
<b>Obligaciones*:</b>	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.
<b>Dirección de Apoyo Normativo a Comités y Contratos</b>	
<b>(Nombre del Usuario 1*)</b>	<b>Lic. Alejandro Martínez Tapia</b>
<b>Cargo*:</b>	<b>Director</b>
<b>Funciones*:</b>	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.
<b>Obligaciones*:</b>	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.

<b>(Nombre del Usuario 2*)</b>	<b>Alejandro César Arzate Villanueva</b>
<b>Cargo*:</b>	<b>Jefe del Departamento de Apoyo Normativo a Adquisiciones</b>
<b>Funciones*:</b>	Realizar la captura, edición, análisis, seguimiento, asignación y consulta de instrumentos consensuales de contratos.
<b>Obligaciones*:</b>	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.
<b>(Nombre del Usuario 3*)</b>	<b>Palemón Albarrán Arce</b>
<b>Cargo*:</b>	<b>Jefe del Departamento de Apoyo Normativo a Obras</b>
<b>Funciones*:</b>	Realizar el análisis y consulta de antecedentes de instrumentos consensuales de contratos y convenios en materia de obras.
<b>Obligaciones*:</b>	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.
<b>(Nombre del Usuario 4*)</b>	<b>Roberto Campos Carreón</b>
<b>Cargo*:</b>	<b>Abogado Auxiliar</b>
<b>Funciones*:</b>	Analizar, buscar, realizar consultas de antecedentes, generar reportes, capturar los instrumentos consensuales.
<b>Obligaciones*:</b>	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.
<b>(Nombre del Usuario 5*)</b>	<b>Gilberto Zambrano Mar</b>
<b>Cargo*:</b>	<b>Secretario Auxiliar</b>
<b>Funciones*:</b>	Analizar, buscar, realizar consultas de antecedentes,

<b>Obligaciones*:</b>	<p>generar reportes, capturar los instrumentos consensuales.</p> <p>Proteger los datos personales de los involucrados en los instrumentos consensuales.</p> <p>No modificar los datos personales contenidos en los instrumentos consensuales.</p> <p>No difundir la información de datos personales contenidos en los instrumentos consensuales.</p> <p>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.</p>
<b>(Nombre del Usuario 6*)</b>	<b>Alfredo Velasco Valerio</b>
<b>Cargo*:</b>	<b>Abogado Auxiliar</b>
<b>Funciones*:</b>	Analizar, buscar, realizar consultas de antecedentes, generar reportes, capturar los instrumentos consensuales.
<b>Obligaciones*:</b>	<p>Proteger los datos personales de los involucrados en los instrumentos consensuales.</p> <p>No modificar los datos personales contenidos en los instrumentos consensuales.</p> <p>No difundir la información de datos personales contenidos en los instrumentos consensuales.</p> <p>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.</p>
<b>(Nombre del Usuario 7*)</b>	<b>Yanina Muñoz López</b>
<b>Cargo*:</b>	<b>Abogada Auxiliar</b>
<b>Funciones*:</b>	Analizar, buscar, realizar consultas de antecedentes, generar reportes, capturar los instrumentos consensuales.
<b>Obligaciones*:</b>	<p>Proteger los datos personales de los involucrados en los instrumentos consensuales.</p> <p>No modificar los datos personales contenidos en los instrumentos consensuales.</p> <p>No difundir la información de datos personales contenidos en los instrumentos consensuales.</p> <p>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.</p>
<b>(Nombre del Usuario 8*)</b>	<b>Adriana López Trinidad</b>
<b>Cargo*:</b>	<b>Asistente ejecutiva</b>
<b>Funciones*:</b>	<p>Analizar, buscar, realizar consultas de antecedentes, generar reportes, capturar los instrumentos consensuales.</p> <p>Administrar los datos de las "contrapartes" señaladas en los instrumentos consensuales.</p> <p>Intercambiar y verificar información con la Dirección de Convenios.</p>
<b>Obligaciones*:</b>	<p>Proteger los datos personales de los involucrados en los instrumentos consensuales.</p> <p>No modificar los datos personales contenidos en los</p>



	<p>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.</p>
<b>Departamento de Enlace de Transparencia</b>	
<b>(Nombre del Usuario 1*)</b>	<b>María Isabel Molina Cigarroa</b>
<b>Cargo*:</b>	<b>Jefa de Departamento</b>
<b>Funciones*:</b>	Consultar los instrumentos consensuales almacenados en el SAGICO.
<b>Obligaciones*:</b>	<p>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.</p>
<b>(Nombre del Usuario 2*)</b>	<b>Montserrat Toci Vargas Vázquez</b>
<b>Cargo*:</b>	<b>Abogada Auxiliar</b>
<b>Funciones*:</b>	Consultar los instrumentos consensuales almacenados en el SAGICO.
<b>Obligaciones*:</b>	<p>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.</p>
<b>(Nombre del Usuario 3*)</b>	<b>Marisol Guevara Arteaga</b>
<b>Cargo*:</b>	<b>Abogada Auxiliar</b>
<b>Funciones*:</b>	Consultar los instrumentos consensuales almacenados en el SAGICO.
<b>Obligaciones*:</b>	<p>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.</p>
<b>(Nombre del Usuario 4*)</b>	<b>Luz Ofelia Sobrado Ramírez</b>
<b>Cargo*:</b>	<b>Abogada Auxiliar</b>
<b>Funciones*:</b>	Consultar los instrumentos consensuales almacenados en el SAGICO.
<b>Obligaciones*:</b>	<p>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.</p>

<b>380 Usuarios Web del Sistema</b>	
<b>Cargo*:</b>	<b>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.</b>
<b>Funciones*:</b>	Consultar, dar seguimiento, generar reportes y/o capturar los instrumentos consensuales en el SAGICO de sus respectivas entidades y dependencias.
<b>Obligaciones*:</b>	Proteger los datos personales de los involucrados en los instrumentos consensuales, no modificarlos, no difundirlos, no realizar alteraciones deliberadamente.

<b>Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General</b>	
<b>Identificador único*</b>	Usuarios
<b>(Nombre del sistema A2) *</b>	Biblioteca "Jorge Carpizo"
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	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.
<b>Responsable*:</b>	
<b>Nombre*:</b>	<b>Ing. Jesús Antonio Sandoval Navarrete</b>
<b>Cargo*:</b>	<b>Responsable de la Biblioteca</b>
<b>Funciones*:</b>	Administrar la base de datos de usuarios.
<b>Obligaciones*:</b>	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.

<b>Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria</b>	
<b>Identificador único*</b>	SAP
<b>(Nombre del sistema A3) *</b>	Sistema Almacén de Publicaciones
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	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.
<b>Responsable*:</b>	
<b>Nombre*:</b>	<b>Ing. Jesús Antonio Sandoval Navarrete</b>
<b>Cargo*:</b>	<b>Jefe del Departamento de Publicaciones</b>

<b>Funciones*:</b>	Consultar la base de datos, capturar los datos del cliente, generar el recibo de dotación, recabar la firma de autorización y entregar la publicación.
<b>Obligaciones*:</b>	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

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

<b>Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General</b>	
<b>Identificador único**</b>	Usuarios
<b>(Nombre del sistema A2*)</b>	Biblioteca "Jorge Carpizo"
<b>Tipo de soporte:*</b>	Físico y electrónico.
<b>Descripción:*</b>	<b>Ver comentario</b>
<b>Características del lugar donde se resguardan los soportes:*</b>	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: 02425483, 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.

<b>Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria</b>	
<b>Identificador único**</b>	SAP
<b>(Nombre del sistema A3*)</b>	Sistema Almacén de Publicaciones
<b>Tipo de soporte:*</b>	Físico y electrónico.
<b>Descripción:*</b>	<b>Ver comentario</b>
<b>Características del lugar donde se resguardan los soportes:*</b>	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: 02425483, con nombre de usuario y contraseña como medida de seguridad, no se tiene acceso a la base de datos desde la red.

Eliminado: dos renglones donde se especifican las características del lugar donde se resguardan los soportes referentes al sistema SAGICO y dos renglones, relacionado con la descripción de soporte referentes a los sistemas Biblioteca "Jorge Carpizo" y SAP. 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.

### 3. ANÁLISIS DE RIESGOS

Departamento de Cómputo y Automatización 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

Eliminado: doce cuadros con descripción correspondientes al Análisis de Riesgo (riesgo, impacto y mitigación), referente al sistema SAGICO. 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

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: veintitrés cuadros con descripción correspondientes al Análisis de Riesgo (riesgo, impacto y mitigación), referente al sistema SAGICO, así como, tres cuadros con descripción correspondientes al Análisis de Riesgo (riesgo, impacto y mitigación), referente al sistema de la Biblioteca "Jorge Carpizo". 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

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

Eliminado: dieciocho cuadros con descripción correspondientes al Análisis de Riesgo (riesgo, impacto y mitigación), referente al sistema de la Biblioteca "Jorge Carpizo", así como, nueve cuadros con descripción al Análisis de Riesgo (riesgo, impacto y mitigación), referente al sistema SAP. 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

#### 4. ANÁLISIS DE BRECHA

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

# Ver comentario

Eliminado: doce cuadros con descripción correspondientes al Análisis de Riesgo (riesgo, impacto y mitigación), referente al sistema de SAP, así como, tres cuadros con descripción correspondiente al Análisis de Brecha (medida de seguridad actual, medida de seguridad necesaria y acciones para remediación) del sistema SAGICO. 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

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

# 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

Eliminado: descripción del análisis de Brecha (medidas de seguridad actual, medidas de seguridad necesaria y acciones para remediación); tres cuadros con descripción referente al sistema SAGICO, seis cuadros con descripción correspondiente al sistema de Biblioteca "Jorge Carpizo" y seis cuadros con descripción correspondiente al sistema SAP. 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.



## 5. PLAN DE TRABAJO

La Dirección General de Estudios de Legislación Universitaria de acuerdo a su presupuesto asignado y al personal con que cuenta en el Departamento de Cómputo y Automatización desarrollará las acciones necesarias para optimizar la seguridad de los sistemas que incluyen y/o dan tratamiento a los datos personales, de conformidad con los resultados del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad conforme a los riesgos reales detectados, de acuerdo al plan de trabajo siguiente:

Departamento de Cómputo y Automatización 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

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

Eliminado: descripción del plan de trabajo (actividad, descripción, duración y cobertura): dieciséis cuadros con descripción referente al sistema SAGICO y ocho cuadros con descripción correspondiente al sistema de Biblioteca "Jorge Carpizo". 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

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

Eliminado: descripción del Plan de Trabajo (actividad, descripción, duración y cobertura): ocho cuadros con descripción correspondiente al sistema de Biblioteca "Jorge Carpizo" y doce cuadros con descripción correspondiente al sistema SAP. 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.

## 6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### I. TRANSFERENCIAS DE DATOS PERSONALES

<b>Departamento de Cómputo y Automatización de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)</b>	
<b>Identificador único*</b>	SAGICO
<b>(Nombre del sistema A1)*</b>	Sistema para la Administración y Gestión de Instrumentos Consensuales
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
<b>Transferencias mediante el traslado de soportes físicos:</b>	No se realizan transferencias de datos personales en soportes físicos.
<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias de datos personales en soportes electrónicos.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No se realizan transferencias de datos personales sobre redes electrónicas.

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

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

<b>Transferencias mediante el traslado de soportes electrónicos:</b>	No se realizan transferencias de datos personales en soportes electrónicos.
<b>Transferencias mediante el traslado sobre redes electrónicas:</b>	No se realizan transferencias de datos personales sobre redes electrónicas.

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

<b>Departamento de Cómputo y Automatización de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)</b>	
<b>Identificador único*</b>	SAGICO
<b>(Nombre del sistema A1)*</b>	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.

### Personal adscrito a la Unidad Administrativa de la DGELU:

Nombre	Cargo	Funciones	Obligaciones
Cristina Alberto Pimentel	Jefa de Unidad Administrativa	Planear, dirigir, coordinar, organizar y controlar los recursos humanos, materiales y financieros con los que cuenta la Dependencia.	Administrar eficientemente los recursos humanos, financieros y materiales asignados., Proporcionar los servicios generales de apoyo a las diferentes áreas que integran la dependencia, Cumplir con las políticas establecidas por la

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.

			Administración Universitaria.
Fernando Sarabia Tránsito	Jefe de Bienes, Suministros y Servicios Generales	Establecer en coordinación con la Jefa de Unidad Administrativa de la dependencia, los programas anuales de adquisiciones y mantenimiento en coordinación con el jefe inmediato de acuerdo al presupuesto autorizado.	Colaborar en la adquisición, contratación y control de bienes y servicios, así como brindar los servicios requeridos para el desempeño de las funciones sustantivas de la dependencia.

**Personal adscrito a la Dirección de Convenios:**

Nombre	Cargo	Funciones	Obligaciones
Cristina Galicia Vázquez	Encargada de despacho	Coordinar la entrada, seguimiento y desahogo de los instrumentos consensuales de contratos y contratos de obra, de conformidad con la Legislación Universitaria. Consultar y generar reportes de los instrumentos consensuales almacenados en el SAGICO.	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.
Karla Gabriela Hernández Andrade	Jefa del Departamento de Instrumentos Consensuales Nacionales	Realizar el seguimiento, consulta de antecedentes y control de los instrumentos consensuales asignados al área de Convenios. Consultar, analizar y	Proteger los datos personales de los involucrados en los instrumentos consensuales. No modificar los datos personales contenidos en los instrumentos consensuales. No difundir la

			generar reportes de los instrumentos consensuales almacenados en el SAGICO.	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.
Cristina Vázquez	Galicia	Jefa del Departamento de Instrumentos Consensuales Internacionales	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.	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.
Erika Suárez	Alejandra Guevara	Secretaria Auxiliar	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	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

		Apoyo Normativo a Comités y Contratos.	contienen datos personales en el servidor de SAGICO y no generar copias de los mismos en su equipo de trabajo.
Eleazar Albarrán Vergara Emmanuel Coraza Pérez Marco Antonio Núñez Campuzano Daniel Alejandro Ramírez García Soledad Iliana Orihuela Aguilar María Alejandra Sánchez Vite Luis Daniel Luna Santacruz Kevin Granados Flores Lizbet Guadalupe Flores Gómez	Abogados y Abogadas Auxiliares	Analizar, buscar y localizar antecedentes, realizar consultas y generar reportes sobre los instrumentos consensuales alojados en el SAGICO.	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.

**Personal adscrito a la Dirección de Apoyo Normativo a Comités y Contratos:**

Nombre	Cargo	Funciones	Obligaciones
Lic. Alejandro Martínez Tapia	Director	Coordinar la entrada, seguimiento y desahogo de los instrumentos consensuales de contratos y contratos de obra, de conformidad con la Legislación Universitaria.  Consultar y generar reportes de los instrumentos consensuales almacenados en el SAGICO.	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.
Alejandro César Arzate Villanueva	Jefe del Departamento de Apoyo Normativo a Adquisiciones	Realizar la captura, edición, análisis, seguimiento, asignación y consulta de instrumentos consensuales de contratos.	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.
Palemón Albarrán Arce	Jefe del Departamento de Apoyo Normativo a Obras	Realizar el análisis y consulta de antecedentes de instrumentos consensuales de contratos de obra.	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.
Roberto Campos Carreón	Abogado Auxiliar	Analizar, buscar, realizar consultas de antecedentes,	Proteger los datos personales de los involucrados en los instrumentos
Alfredo Velasco	Abogado Auxiliar	generar reportes,	

<p>Valerio</p> <p>Yanina Muñoz López</p> <p>Gilberto Zambrano Mar</p>	<p>Abogada Auxiliar</p> <p>Secretario Auxiliar</p>	<p>capturar los instrumentos consensuales.</p>	<p>consensuales.</p> <p>No modificar los datos personales contenidos en los instrumentos consensuales.</p> <p>No difundir la información de datos personales contenidos en los instrumentos consensuales.</p> <p>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.</p>
<p>Adriana López Trinidad</p>	<p>Asistente ejecutiva</p>	<p>Analizar, buscar, realizar consultas de antecedentes, generar reportes, capturar los instrumentos consensuales.</p> <p>Administrar los datos de las "contrapartes" señaladas en los instrumentos consensuales.</p> <p>Intercambiar y verificar información con la Dirección de Convenios.</p>	<p>Proteger los datos personales de los involucrados en los instrumentos consensuales.</p> <p>No modificar los datos personales contenidos en los instrumentos consensuales.</p> <p>No difundir la información de datos personales contenidos en los instrumentos consensuales.</p> <p>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.</p>

### 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.

Ver comentario

2. Si las bitácoras están en soporte físico o en soporte electrónico;

Ver comentario

3. Lugar dónde almacena las bitácoras y por cuánto tiempo;

Ver comentario

4. La manera en que asegura la integridad de las bitácoras, y

Ver comentario

5. 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

Ver comentario

- 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

Eliminado: catorce renglones 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.

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?

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?  
Sí.

b)  Ver comentario

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?

El Jefe 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?

Sí, se encuentran contenidos en la base de datos de sistema.

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 lo requieren.

b)  Ver comentario

c)  Ver comentario

## 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; <sup>1</sup>

3. Disco duro.

4.  Ver comentario

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

<sup>1</sup> 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.

## IX. PLAN DE CONTINGENCIA

# Ver comentario

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

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

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.

Nombre	Cargo	Funciones	Obligaciones
Jesús Antonio Sandoval Navarrete	Responsable de Biblioteca	Administrar la base de 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.

#### 2. Si las bitácoras están en soporte físico o en soporte electrónico;

#### 3. Lugar dónde almacena las bitácoras y por cuánto tiempo;

#### 4. La manera en que asegura la integridad de las bitácoras, y

#### 5. 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 consignent 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.

### 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 ha 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;<sup>2</sup>

3. Se utiliza disco duro SSD o memoria USB.

**Ver comentario**

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

**IX. PLAN DE CONTINGENCIA**

**Ver comentario**

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

<sup>2</sup> 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.

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

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

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

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.

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.

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	Jefe del Departamento de Publicaciones	Administrar la base de 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 solicitan 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 solicitantes los nombres de usuario y contraseñas de acceso al SAGICO.	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.

### **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.
2. Si las bitácoras están en soporte físico o en soporte electrónico;
  3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
  4. La manera en que asegura la integridad de las bitácoras, y
  5. 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 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 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;<sup>3</sup>  
Se utiliza disco duro SSD o memoria USB.

Ver comentario

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

## IX. PLAN DE CONTINGENCIA

Ver comentario

<sup>3</sup> 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 Trigesimo primero de los Lineamientos; o bien, si utiliza un espacio externo seguro para guardar de manera sistemática dichos respaldos, según la fracción VIII del Trigesimo séptimo de tales Lineamientos.



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

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

<b>Departamento de Cómputo y Automatización de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)</b>		
<b>Identificador único*</b>	SAGICO	
<b>(Nombre del sistema A1)*</b>	Sistema para la Administración y Gestión de Instrumentos Consensuales	
<b>Recurso*</b>	<b>Descripción*</b>	<b>Control*</b>
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: Mtro. Hans Kohler Lizardi.
Firewall actualizado.	Revisar periódicamente el Firewall para verificar que se encuentre actualizado y no tenga alguna alerta de seguridad.	Licencia anual Responsable: Mtro. Hans Kohler Lizardi.

<b>Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General</b>		
<b>Identificador único*</b>	Usuarios	
<b>(Nombre del sistema A2)*</b>	Biblioteca "Jorge Carpizo"	
<b>Recurso*</b>	<b>Descripción*</b>	<b>Control*</b>
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.

<b>Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria</b>		
<b>Identificador único*</b>	SAP	

<b>(Nombre del sistema A3)*</b>	Sistema Almacén de Publicaciones	
<b>Recurso*</b>	<b>Descripción*</b>	<b>Control*</b>
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

<b>Departamento de Cómputo y Automatización de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)</b>		
<b>Identificador único*</b>	SAGICO	
<b>(Nombre del sistema A1)*</b>	Sistema para la Administración y Gestión de Instrumentos Consensuales	
<b>Medida de seguridad*</b>	<b>Procedimiento*</b>	<b>Responsable*</b>
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: Mtro. Hans Kohler Lizardi. 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: Mtro. Hans Kohler Lizardi. 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: Mtro. Hans Kohler Lizardi. Tiempo: 1 día

<b>Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General</b>		
<b>Identificador único*</b>	Usuarios	
<b>(Nombre del sistema A2)*</b>	Biblioteca "Jorge Carpizo"	
<b>Medida de seguridad*</b>	<b>Procedimiento*</b>	<b>Responsable*</b>
Seguridad de los datos personales de los usuarios	Comprobar que el equipo cuenta con las	a) El Departamento de Cómputo y Automatización.

resguardados en el equipo de cómputo del responsable de la biblioteca.	actualizaciones correspondientes, en cuanto al software o hardware.	b) 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**

<b>Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria</b>		
<b>Identificador único*</b>	SAP	
<b>(Nombre del sistema A3)*</b>	Sistema Almacén de Publicaciones	
<b>Medida de seguridad*</b>	<b>Procedimiento*</b>	<b>Responsable*</b>
Seguridad de los datos personales de los usuarios resguardados en el equipo de cómputo del jefe del Departamento de Publicaciones.	Comprobar que el equipo cuenta con las actualizaciones correspondientes, en cuanto al software o hardware.	a) El Departamento de Cómputo y Automatización. b) 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

<b>Departamento de Cómputo y Automatización de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)</b>		
<b>Identificador único*</b>	SAGICO	
<b>(Nombre del sistema A1)*</b>	Sistema para la Administración y Gestión de Instrumentos Consensuales	
<b>Medida de seguridad*</b>	<b>Resultado de evaluación*</b>	<b>Responsable*</b>
Actualizar listado de usuarios activos.	Los permisos de usuario se encuentran actualizados.	Responsable: Mtro. Hans Kohler Lizardi.
Actualizar el software	El software se encuentra	Responsable:

Eliminado: descripción de procedimiento para la revisión de las medidas de seguridad; tres cuadros con descripción correspondientes al sistema de la Biblioteca "Jorge Carpizo" y tres cuadros con descripción al sistema SAP. 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.

antivirus y antimalware del Firewall.	actualizado y se está gestionando la renovación de la licencia para que la protección continúe.	Mtro. Hans Kohler Lizardi.
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: Mtro. Hans Kohler Lizardi.

<b>Biblioteca "Jorge Carpizo" de la Oficina de la Abogacía General</b>		
<b>Identificador único*</b>	Usuarios	
<b>(Nombre del sistema A2)*</b>	Biblioteca "Jorge Carpizo"	
<b>Medida de seguridad*</b>	<b>Resultado de evaluación*</b>	<b>Responsable*</b>
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.

<b>Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria</b>		
<b>Identificador único*</b>	SAP	
<b>(Nombre del sistema A3)*</b>	Sistema Almacén de Publicaciones	
<b>Medida de seguridad*</b>	<b>Resultado de evaluación*</b>	<b>Responsable*</b>
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

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

Medida de seguridad*	Acciones*	Responsable*
----------------------	-----------	--------------

# 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: descripción de las acciones para la corrección y actualización de las medidas de seguridad: nueve cuadros con descripción, referente al sistema SAGICO y tres cuadros con descripción correspondientes al sistema SAP. 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.

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

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

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

<b>Actividad*</b>	<b>Descripción*</b>	<b>Duración*</b>	<b>Cobertura*</b>
Programa de capacitación sobre protección de datos personales.	Curso en línea.	1 al 5 de abril de 2024, 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	1 al 5 de abril de 2024, 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 frecuencia de actualización.

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

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

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

<b>Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria</b>	
<b>Identificador único*</b>	SAP
<b>(Nombre del sistema A3)*</b>	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

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

# 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 y Automatización 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*

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.



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 capacidad de procesamiento y almacenamiento del equipo.	Las actualizaciones dependerán de los recursos asignados y, en su caso, se efectúan a equipos considerados críticos.  Dos días.	Se reduce al mínimo el riesgo de pérdida de datos por falla del equipo.

<b>Biblioteca “Jorge Carpizo” de la Oficina de la Abogacía General</b>	
<b>Identificador único*</b>	Usuarios
<b>(Nombre del sistema A2)*</b>	Biblioteca “Jorge Carpizo”

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

Conforme a lo dispuesto en el Programa de Racionalidad Presupuestal 2023 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

<b>Departamento de Cómputo y Automatización de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)</b>		
<b>Identificador único*</b>	SAGICO	
<b>(Nombre del sistema A1)*</b>	Sistema para la Administración y Gestión de Instrumentos Consensuales	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
Respaldo de la base de datos del sistema.	El respaldo se lleva a cabo diariamente y se almacena en	Responsables: Mtro. Hans Kohler Lizardi.

	un medio diferente al servidor para su conservación en caso de alguna eventualidad.	Ing. David Ricardo Montalván Rodríguez.
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: Mtro. Hans Kohler Lizardi.

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

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

<b>Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria</b>	
<b>Identificador único*</b>	SAP
<b>(Nombre del sistema A3)*</b>	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

<b>Departamento de Cómputo y Automatización de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)</b>		
<b>Identificador único*</b>	SAGICO	
<b>(Nombre del sistema A1)*</b>	Sistema para la Administración y Gestión de Instrumentos Consensuales	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
Disposición final de equipos o componentes de cómputo.	<ol style="list-style-type: none"> <li>1. El Departamento de Cómputo y Automatización genera el listado de los equipos destinados a la baja.</li> <li>2. La Unidad Administrativa de la DGELU verifica los equipos inventariables y de control interno.</li> <li>3. Se recibe la autorización de la Unidad Administrativa.</li> <li>4. Se solicita a la Dirección General de Patrimonio la baja y se programa una visita</li> </ol>	Unidad Administrativa.

	<p>por para verificar el estado físico de los equipos.</p> <p>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.</p> <p>6. Se realiza la entrega física de los equipos con documentos de entrega-recepción.</p> <p>7. Se concluye el proceso eliminando los equipos del Sistema de Control Patrimonial (SICOP).</p>	
--	--	--

<b>Biblioteca “Jorge Carpizo” de la Oficina de la Abogacía General</b>		
<b>Identificador único*</b>	<b>Usuarios</b>	
<b>(Nombre del sistema A2)*</b>	<b>Biblioteca “Jorge Carpizo”</b>	
<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
Disposición final de equipos o componentes de cómputo.	<ol style="list-style-type: none"> <li>1. El Departamento de Cómputo y Automatización genera el listado de los equipos destinados a la baja.</li> <li>2. La Unidad Administrativa de la DGELU verifica los equipos inventariables y de control interno.</li> <li>3. Se recibe la autorización de la Unidad Administrativa.</li> <li>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.</li> <li>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.</li> <li>6. Se realiza la entrega física de los equipos con documentos de entrega-recepción.</li> <li>7. Se concluye el proceso eliminando los equipos del Sistema de Control Patrimonial (SICOP).</li> </ol>	Unidad Administrativa.

<b>Departamento de Publicaciones de la Dirección General de Estudios de Legislación Universitaria</b>	
<b>Identificador único*</b>	SAP

<b>(Nombre del sistema A3)*</b>	Sistema Almacén de Publicaciones
---------------------------------	----------------------------------

<b>Proceso*</b>	<b>Descripción*</b>	<b>Responsable*</b>
Disposición final de equipos o componentes de cómputo.	<ol style="list-style-type: none"> <li>1. El Departamento de Cómputo y Automatización genera el listado de los equipos destinados a la baja.</li> <li>2. La Unidad Administrativa de la DGELU verifica los equipos inventariables y de control interno.</li> <li>3. Se recibe la autorización de la Unidad Administrativa.</li> <li>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.</li> <li>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.</li> <li>6. Se realiza la entrega física de los equipos con documentos de entrega-recepción.</li> <li>7. Se concluye el proceso eliminando los equipos del Sistema de Control Patrimonial (SICOP).</li> </ol>	Unidad Administrativa.

Ver comentario

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

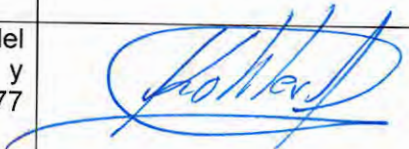


<b>11. Departamento de Cómputo y Automatización de la Dirección de Documentación y Difusión de la Dirección General de Estudios de Legislación Universitaria (DGELU)</b>	
<b>Identificador único*</b>	SAGICO
<b>(Nombre del sistema A1)*</b>	Sistema para la Administración y Gestión de Instrumentos Consensuales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

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.

<b>Identificador único*</b>	SAP
<b>(Nombre del sistema A3)*</b>	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:
<b>Responsable desarrollo:</b>	<b>del</b>	
	Mtro. Hans Kohler Lizardi, Jefe del Departamento de Cómputo y Automatización, tel. (55) 5622-6377 Ext. 48077, hkohler@unam.mx	
	Ing. J. Antonio Sandoval Navarrete, Jefe del Departamento de Publicaciones, tel. (55) 5622-6377 Ext. 82573, jasan@unam.mx	
<b>Revisó:</b>	Lic. Rafael González Zaldivar, Director de Documentación y Difusión, (55) 5622-6377 Ext. 48071, ragonzal@unam.mx	
<b>Autorizó:</b>	Dra. Ángela Quiroga Quiroga, Directora General de Estudios de Legislación Universitaria, tel. (55) 5622-6371 Ext. 48085, dgelu@unam.mx	
<b>Fecha de aprobación:</b>	(Incluir la fecha de liberación del documento)	16 de enero de 2024
<b>Fecha de actualización:</b>	(Incluir la primer versión e ir agregando las subsiguientes del documento)	16 de enero de 2024

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 referentes al Sistema para la Administración y Gestión de Instrumentos Consensuales (SAGICO) y un renglón, relacionado con la descripción de soporte referente del Sistema de la Biblioteca "Jorge Carpizo" y dos del Sistema Almacén de Publicaciones (SAP), pág. 19; Análisis de Riesgo págs. 20 - 23; Análisis de Brecha págs. 23 y 24; Plan de Trabajo, págs. 25 - 27; Medidas de seguridad, once renglones, pág. 29, catorce renglones, pág. 35, diez renglones, pág. 38, dieciocho renglones, pág. 39, trece renglones, pág. 43 y diecisiete renglones, pág. 48; Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad: tres cuadros con descripción 51 y nueve cuadros con descripción, pág. 53; Mejora Continua: ocho cuadros con descripción pág. 56 y dos renglones pág. 60.

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 obstruya la prevención o persecución de los delitos.

Periodo de reserva: 5 años, los cuales se computarán a partir de la fecha de la resolución.

Fecha y número de acta de la sesión: 19/08/2022 y CTUNAM/525/2022.

