UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
OFICINA DE LA ABOGACÍA GENERAL
DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Ciudad Universitaria, Cd. Mx., a 12 de agosto de 2022

***VERSIÓN PÚBLICA**

ÍNDICE

INTRODUCCIÓN

Derivado de la reforma constitucional de 2014 en materia de transparencia, en enero de 2017, se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General) que tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de Sujetos Obligados. En este nuevo esquema se reconoce a la Universidad Nacional Autónoma de México como Sujeto Obligado para cumplir con los principios, deberes y demás obligaciones reconocidos por dicha Ley.

Bajo este contexto, en específico en el artículo 35 de la Ley General, se establece la necesidad de documentar las medidas de seguridad con que cuenta cada Sujeto Obligado para la protección de los datos personales en su posesión, esto a través de un documento de seguridad, el cual es definido como aquel instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales a los cuales da tratamiento.

Al respecto, el numeral citado señala como requisitos mínimos que el documento de seguridad debe contener, los siguientes:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

Con base en lo anterior, el presente documento define los criterios, controles y programas de seguimiento y supervisión de manera genérica, respecto de las medidas de seguridad técnicas, físicas y administrativas adoptadas por la Dirección General de Asuntos Jurídicos (DGAJ), para garantizar la protección de los datos personales que obran en su Sistema de Gestión de Asuntos Recibidos (SIGAR).

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES.

En el presente apartado se identificará el tratamiento de datos personales que lleva a cabo la DGAJ, por lo que contiene la información básica del mismo, con la finalidad de contar con un control documentado, preciso y ordenado, integrándose de la siguiente manera:

- El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;
- Las finalidades de cada tratamiento de datos personales;
- El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;
- El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales; y
- La lista de trabajadores universitarios que tienen acceso al sistema de tratamiento.

SISTEMA DE GESTIÓN DE ASUNTOS RECIBIDOS (SIGAR)

El SIGAR, es un sistema de control y seguimiento para la correspondencia que se recibe diariamente en la DGAJ a través de la Oficialía de Partes y vía electrónica. Dicho sistema permite registrar y ordenar todos los asuntos que ingresan, así como proporcionar una búsqueda eficiente para su localización.

El objetivo principal del SIGAR es contar con el registro de cada uno de la correspondencia, el cual contiene los datos generales más relevantes, que permitan su localización en caso de ser necesario, así como el respectivo trámite otorgado para su atención; así también, tiene como propósito hacer más eficiente la comunicación y el flujo de información entre las diferentes direcciones, departamentos y áreas que conforman esta DGAJ, logrando de esta manera desahogar con mayor celeridad los asuntos, reduciendo los tiempos de turnado.

1.1.- Datos personales que se tratan y Finalidades del tratamiento.

Dato Personal (sensibles o no) contenidos en el sistema	Finalidad
• Afiliación sindical. • Afores. • Bienes muebles e inmuebles. • Cadena original del complemento de certificación digital del SAT.	Brindar la atención que corresponda de acuerdo con las atribuciones y funciones que tiene conferidas la DGAJ, en materia de representación legal ante las instancias judiciales, administrativas y ministeriales, federales y locales, así como asesorar jurídicamente a las autoridades

Dato Personal (sensibles o no) contenidos en el sistema	Finalidad
• Calificaciones que permiten conocer el aprovechamiento académico de una persona, así como los avances de créditos, tipos de exámenes, promedio, y trayectoria. • Características físicas (rasgos fisonómicos o media filiación de una persona). • Cartilla militar. • Cédula profesional. • Certificado de sello digital - Servicio de Administración Tributaria (SAT). • Certificados y reconocimientos, entre otros. • Clave de elector. • Clave única del registro de población (CURP). • Código postal. • Correo electrónico personal. • Costumbres. • Creencias religiosas, filosóficas y morales. • Cuenta bancaria, número de cuenta bancaria y/o clave bancaria estandarizada (CLABE) de personas físicas. • Cuenta catastral. • Cuotas sindicales. • Dependientes y beneficiarios económicos. • Descuentos personales contenidos en recibos de pago. • Domicilio particular. • Edad. • Estado civil. • Estado de salud presente o futuro (historial clínico, alergias, enfermedades, información	administrativas y universitarias y a los órganos colegiados.

Dato Personal (sensibles o no) contenidos en el sistema	Finalidad
relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, grupo sanguíneo o tipo de sangre, entre otros) y capacidades diferentes. • Fecha de nacimiento. • Firma electrónica, siempre y cuando se desprendan datos personales. • Firma o rúbrica de particulares. • Folio fiscal de facturas expedidas por personas físicas. • Fotografías de personas. • Historial crediticio. • Huella digital. • Idioma, lengua o dialecto. • Información fiscal. • Información genética. • Información relacionada con el patrimonio de una persona física. • Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros. • Ingresos y egresos. • Lugar de nacimiento. • Matrícula del servicio militar. • Montos aportados al seguro de separación individualizado. • Nacionalidad. • Nombre de personas físicas. • Nombres de familiares, dependientes y beneficiarios.	

Dato Personal (sensibles o no) contenidos en el sistema	Finalidad
• Número de cuenta o número de matrícula escolar. • Número de pasaporte. • Número de póliza de seguro. • Número de seguridad social. • Número de seguro de separación individualizado. • Número de teléfono fijo y celular (personal). • Número de visa. • Origen racial o étnico. • Parentesco (filiación). • Participación societaria y nombre de socios, contenidos en documentos notariados, tales como escrituras públicas, estatutos, contratos y convenios privados. • Preferencia sexual. • Preferencias políticas. • Profesión u ocupación. • Redes sociales (información relacionada con publicaciones en redes sociales de personas físicas). • Referencias laborales. • Referencias familiares y/o personales. • Registro federal de contribuyentes (RFC). • Secretos comerciales, industriales, fiscales, bancarios y fiduciarios. • Seguros. • Sello del comprobante fiscal digital por internet (CFDI). • Sello digital y/o código bidimensional. • Sexo.	

1.2.- Medios de obtención de los datos personales.

Forma de obtención de los datos personales	Directa o indirecta
Medio físico y electrónico	Indirecta

1.3. Tipo de soporte y descripción general de donde se resguarda el sistema.

Tipo de soporte	Electrónico y físico
Ubicación donde se resguarda	Los datos en formato electrónico se encuentran en un servidor que se aloja en el cuarto de comunicaciones de la DGAJ resguardado y monitoreado continuamente y respecto del soporte físico en un espacio asignado para archivo de la propia Dirección General.

1.4. Funciones y obligaciones de personas trabajadoras universitarias que tienen acceso al sistema.

Responsable 1:	
Nombre:	**MARTÍNEZ MÚÑOZ LIZBETH BETZAI**
Cargo:	Coordinadora de Gestión de la DGAJ
Funciones:	• Registrar en el SIGAR la correspondencia recibida de manera física y/o electrónica la cual pudiera contener datos personales. • Supervisar el tratamiento de datos personales contenidos en el SIGAR. • Resguardar física y/o electrónicamente los datos personales recabados en el SIGAR, hasta en tanto se turne a las áreas competentes. • Emitir y coordinar las medidas necesarias a fin de salvaguardar y evitar cualquier vulneración a la seguridad de los datos personales en el SIGAR. • Transferir la correspondencia en el SIGAR, al área que corresponda para su conocimiento, atención, desahogo y/o seguimiento según sea el caso. • Dar seguimiento al estatus que guardan los asuntos turnados en el SIGAR.

Responsable 1:	
	• Gestionar la generación de los reportes necesarios para el debido funcionamiento del SIGAR.
Obligaciones:	• Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la normativa universitaria. • Adoptar las medidas necesarias para garantizar la confidencialidad de la información y los documentos que integran el SIGAR. • Informar al responsable técnico de datos personales de la Dirección General, cuando ocurra o se detecte una probable vulneración a los datos personales. • Cumplir con las medidas de seguridad implementadas por la Dirección General.

Responsable 2:	
Nombre:	**VÁZQUEZ DÍAZ ARMANDO**
Cargo:	Jefe del Departamento de Informática
Funciones:	• Actualizar y asignar privilegios a los usuarios del SIGAR. • Apoyar en búsquedas de asuntos registrados en el SIGAR. • Generar reportes. • Implementar las medidas de seguridad para la protección de los datos personales. • Informar al Director General cuando ocurra una vulneración a los datos personales. • Dar mantenimiento a la base de datos del SIGAR. • Desarrollar la funcionalidad solicitada en el SIGAR. • Mantener siempre disponible la información para los usuarios del SIGAR.
Obligaciones:	• Adoptar las medidas necesarias para garantizar la confidencialidad de la información y los documentos que integran el SIGAR. • Resguardar y controlar el acceso mediante usuario y contraseña que le sea asignado.

Responsable 2:	
	• Fungir como el responsable del funcionamiento técnico del SIGAR. • Proteger los datos personales contenidos en el SIGAR de accesos no autorizados. • Instrumentar políticas para la protección de los datos personales en los servidores y bases de datos de la Dirección General. • Generar los respaldos de la información contenida en el SIGAR. • No modificar los datos personales del SIGAR. • Gestionar las autorizaciones para facultar a un funcionario o trabajador universitario como usuario del SIGAR. • Cumplir con las medidas de seguridad implementadas por la Dirección General.

Encargado:	
Nombre del Encargado:	**NO aplica, no se cuenta con instrumentos consensuales suscritos con terceros.**
Cargo:	
Funciones:	
Obligaciones:	

Administrador:	
Nombre:	**BARRERA GUTIÉRREZ JORGE**
Cargo:	Director General de Asuntos Jurídicos
Funciones:	• Consultar el SIGAR para el seguimiento correspondiente del resto de los usuarios. • Turnar a los directores y encargados de área de la DGAJ los asuntos de su competencia para atenderlos.
Obligaciones:	• Adoptar las medidas necesarias para garantizar la confidencialidad de la información y los documentos que integran el SIGAR. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • No modificar los datos personales del SIGAR. • Proteger los datos personales contenidos en los documentos que ingresan a la Dirección General.

Administrador:	
	• Abstenerse de tratar los datos personales para finalidades distintas a las que tiene encomendadas. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar al responsable técnico de datos personales de la Dirección General cuando se tenga conocimiento de una presunta vulneración a los datos personales.

Usuarios:	
Nombre del Usuario 1	**GARCÍA SERRANO SALVADOR**
Cargo:	ASISTENTE DE PROCESOS
Funciones:	• Recibir, registrar y capturar en el SIGAR la correspondencia que de manera física se presente en la oficialía de partes de la DGAJ. • Registrar y capturar en el SIGAR la correspondencia que llega de manera electrónica. • Registrar y capturar en el SIGAR la correspondencia recibida con el número consecutivo de volante. • Transferir los asuntos capturados a la Coordinación de Gestión, a través del SIGAR, para su transferencia al área correspondiente.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Proteger los datos personales contenidos en los documentos que ingresan a la Dirección General. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Cumplir con las medidas de seguridad implementadas por la Dirección General.

Usuarios:	
Nombre del Usuario 2	**ARMENDÁRIZ LÓPEZ JESÚS ALFREDO**
Cargo:	Director de Asuntos Jurídicos
Funciones:	• Supervisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Coordinar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Conocer y turnar los asuntos de su competencia, al personal a su cargo y, en su caso, consultar los asuntos en el SIGAR. • Coordinar el resguardo físico y/o electrónico de los datos personales recabados en los documentos a que tiene acceso. • Dar seguimiento a la atención de los asuntos que le sean turnados a través del SIGAR.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Proteger los datos personales contenidos en los documentos que ingresan al área a su cargo. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la persona titular de la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar al responsable técnico de datos personales de la Dirección General cuando ocurra o detecte una posible vulneración a los datos personales.
Nombre del Usuario 3	**ARMENDÁRIZ LÓPEZ JESÚS ALFREDO**
Cargo:	Encargado de la Dirección de Asuntos Laborales Contenciosos.

Usuarios:	
Funciones:	• Supervisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Coordinar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Conocer y turnar los asuntos de su competencia, al personal a su cargo y, en su caso, consultar los asuntos en el SIGAR. • Coordinar el resguardo físico y/o electrónico de los datos personales recabados en los documentos a que tiene acceso. • Dar seguimiento a la atención de los asuntos que le sean turnados a través del SIGAR.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Proteger los datos personales contenidos en los documentos que ingresan al área a su cargo. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la persona titular de la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar al responsable técnico de datos personales de la Dirección General cuando ocurra o detecte una posible vulneración a los datos personales.
Nombre del Usuario 4	**CORONEL RIVERA YESICA MARIBEL**
Cargo:	Directora de Propiedad Intelectual
Funciones:	• Supervisar el tratamiento de los datos personales de los asuntos que le sean turnados.

Usuarios:	
	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Coordinar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Conocer y turnar los asuntos de su competencia, al personal a su cargo y, en su caso, consultar los asuntos en el SIGAR. • Coordinar el resguardo físico y/o electrónico de los datos personales recabados en los documentos a que tiene acceso. • Dar seguimiento a la atención de los asuntos que le sean turnados a través del SIGAR.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Proteger los datos personales contenidos en los documentos que ingresan al área a su cargo. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la persona titular de la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar al responsable técnico de datos personales de la Dirección General cuando ocurra o detecte una posible vulneración a los datos personales.
Nombre del Usuario 5	**LUGO CALLEJA INOCENTE**
Cargo:	COORDINADOR DE APOYO AL COMITÉ DE TRANSPARENCIA
Funciones:	• Supervisar el tratamiento de los datos personales de los asuntos que le sean turnados.

Usuarios:	
	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Coordinar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Conocer y turnar los asuntos de su competencia, al personal a su cargo y, en su caso, consultar los asuntos en el SIGAR. • Coordinar el resguardo físico y/o electrónico de los datos personales recabados en los documentos a que tiene acceso. • Dar seguimiento a la atención de los asuntos que le sean turnados a través del SIGAR.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Proteger los datos personales contenidos en los documentos que ingresan al área a su cargo. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la persona titular de la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar al responsable técnico de datos personales de la Dirección General cuando ocurra o detecte una posible vulneración a los datos personales.
Nombre del Usuario 6	**PÉREZ OLIVARES MARY TRINY**
Cargo:	SECRETARIA DE PLANEACIÓN
Funciones:	• Supervisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos.

Usuarios:	
	• Coordinar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Conocer y turnar los asuntos de su competencia, al personal a su cargo y, en su caso, consultar los asuntos en el SIGAR. • Coordinar el resguardo físico y/o electrónico de los datos personales recabados en los documentos a que tiene acceso. • Dar seguimiento a la atención de los asuntos que le sean turnados a través del SIGAR.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Proteger los datos personales contenidos en los documentos que ingresan al área a su cargo. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la persona titular de la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar al responsable técnico de datos personales de la Dirección General cuando ocurra o detecte una posible vulneración a los datos personales.
Nombre del Usuario 7	**QUIROGA GAMBOA JOSE CARLOS**
Cargo:	FUNCIONARIO JEFE UNIDAD ADMINISTRATIVA
Funciones:	• Supervisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Coordinar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales.

Usuarios:	
	• Conocer y turnar los asuntos de su competencia, al personal a su cargo y, en su caso, consultar los asuntos en el SIGAR. • Coordinar el resguardo físico y/o electrónico de los datos personales recabados en los documentos a que tiene acceso. • Dar seguimiento a la atención de los asuntos que le sean turnados a través del SIGAR.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Proteger los datos personales contenidos en los documentos que ingresan al área a su cargo. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la persona titular de la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar al responsable técnico de datos personales de la Dirección General cuando ocurra o detecte una posible vulneración a los datos personales.
Nombre del Usuario 8	**HERNÁNDEZ SERRANO MARTHA LEONOR**
Cargo:	JEFA DEL DEPARTAMENTO DE ASUNTOS CIVILES
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR.

Usuarios:	
	• Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 9	**CORREA GARCÍA I. ADRIÁN**
Cargo:	JEFE DEL DEPARTAMENTO DE ASUNTOS PENALES
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.

Usuarios:	
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 10	**JUÁREZ NAVARRETE VICTOR PABLO**
Cargo:	JEFE DEL DEPARTAMENTO DE AMPAROS
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General.

Usuarios:	
	• Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 11	**FLORES LÓPEZ IRMA LAURA**
Cargo:	JEFA DE LA UNIDAD DE APOYO JURÍDICO
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General.

Usuarios:	
	• Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 12	**VILLALPANDO ROJAS LAURA OLIVIA**
Cargo:	JEFA DEL DEPARTAMENTO DE ASUNTOS ADMINISTRATIVOS
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 13	**ACOSTAVIQUES ORTIZ JORGE**
Cargo:	JEFE DEL DEPARTAMENTO CONTENCIOSO LABORAL

Usuarios:	
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 14	**VÁZQUEZ ARENAS JORGE ANTONIO**
Cargo:	JEFE DEL DEPARTAMENTO DE PROCEDIMIENTO DE INVESTIGACIÓN ADMINISTRATIVA
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a

Usuarios:	
	fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 15	**HIDALGO LEÓN PAMELA JATZIRI**
Cargo:	JEFA DEL DEPARTAMENTO DE CONSULTORÍA Y ESTUDIOS LABORALES
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR.

Usuarios:	
	• Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 16	**GONZÁLEZ REYES RAFAEL**
Cargo:	JEFE DEL DEPARTAMENTO DE CONSULTORÍA PROCESAL A OFICINAS JURÍDICAS
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información.

Usuarios:	
	• Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 17	**CERVANTES PÉREZ IRMA**
Cargo:	JEFA DEL DEPARTAMENTO DE VERIFICACIÓN DE ACTAS
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no

Usuarios:	
	autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 18	**BORJA CHÁVEZ CARLOS MANUEL**
Cargo:	JEFE DEL DEPARTAMENTO DE DERECHOS DE AUTOR
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General.

Usuarios:	
	• Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 19	**FIGUEROA PÉREZ MARTHA**
Cargo:	JEFA DEL DEPARTAMENTO DE PROPIEDAD INDUSTRIAL Y TRANSFERENCIA DE TECNOLOGÍA
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.

Usuarios:	
Nombre del Usuario 20	**FUENTES BALDERAS MARY CARMEN**
Cargo:	JEFA DEL DEPARTAMENTO DE CONVENIOS Y CONTRATOS
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 21	**ROSALES VELASCO DIEGO ARMANDO**
Cargo:	JEFE DEL DEPARTAMENTO DE CÓMITE DE TRANSPARENCIA
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos

Usuarios:	
	personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 22	**GARCÍA TOVAR MIGUEL ÁNGEL**
Cargo:	JEFE DEL DEPARTAMENTO DE DATOS PERSONALES
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le

Usuarios:	
	sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 23	**GERVACIO VENTURA MARILÚ**
Cargo:	JEFA DEL DEPARTAMENTO DE RECURSOS DE REVISIÓN INAI
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.

Usuarios:	
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 24	**SILIS FILIGRANA KARLA LETICIA**
Cargo:	JEFA DEL DEPARTAMENTO DE CONTROL Y SEGUIMIENTO
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la

Usuarios:	
	Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 25	**RAMÍREZ OLVERA KARINA**
Cargo:	JEFA DEL DEPARTAMENTO DE PRESUPUESTO Y PERSONAL
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General.

Usuarios:	
	• Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 26	**JÁUREGUI VARGAS MÓNICA N.**
Cargo:	JEFA DEL DEPARTAMENTO DE BIENES Y SUMINISTROS
Funciones:	• Revisar el tratamiento de los datos personales de los asuntos que le sean turnados. • Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite y seguimiento a los asuntos que le sean asignados a través del SIGAR. • Realizar proyectos de contestación a los asuntos asignados en el SIGAR. • Turnar los asuntos al personal a su cargo. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 27	**ARAGON SANCHEZ OMAR ALBERTO**
Cargo:	SECRETARIO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos

Usuarios:	
	personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 28	**HERNANDEZ BUENROSTRO MARCELA**
Cargo:	SECRETARIO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los

Usuarios:	
	asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 29	**PICHARDO MARTINEZ ALMA BLANCA**
Cargo:	SECRETARIO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su

Usuarios:	
	encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 30	**RUBIO LICONA URSULA ILIANA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 31	**ROSAS DELGADO JESÚS MANUEL**
Cargo:	ABOGADO AUXILIAR

Usuarios:	
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 32	**UGALDE MEDINA AZALEA IRAIS**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR.

Usuarios:	
	• Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 33	**SAGUILÁN LÓPEZ ALMA ANDREA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no

Usuarios:	
	autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 34	**ERCULANO VIDAL PEDRO**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 35	**BERROCAL GONZÁLEZ NALLELI**
Cargo:	ABOGADA AUXILIAR

Usuarios:	
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 36	**LOZANO RAMÍREZ JOSÉ RAMÓN**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR.

	Usuarios:
	• Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 37	**ORTIZ DE LA PAZ ÁNGEL ABEL**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no

Usuarios:	
	autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 38	**OCHOA HERMENEGILDO RODOLFO**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 39	**MORALES ZERMEÑO CAROLINA MONSERRAT**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos

Usuarios:	
	personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 40	**RODRÍGUEZ GONZÁLEZ NORMA ELISA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los

Usuarios:	
	asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 41	**GUTIÉRREZ DIAZ ROBERTO CARLOS**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su

Usuarios:	
	encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 42	**SALAZAR CURIEL BRUNO CESAR**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 43	**VILLAGÓMEZ PELAEZ FRANCISCO MIGUEL**
Cargo:	ABOGADO AUXILIAR

Usuarios:	
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 44	**CORTÉS HERNÁNDEZ IRVIN YADIR**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR.

Usuarios:	
	• Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 45	**BÁRCENAS VALENCIA JOCELIN**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no

Usuarios:	
	autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 46	**MEJÍA LECHUGA VERÓNICA ALEJANDRA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 47	**BECERRIL CORDOVA LIZETH**
Cargo:	ABOGADA AUXILIAR

Usuarios:	
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 48	**TREJO CASTILLO ALFREDO**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR.

Usuarios:	
	• Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 49	**CERÓN ROMERO JOSUÉ IRVING**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no

Usuarios:	
	autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 50	**BRINDIZ ESTIUBARTE OMAR**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 51	**PALACIOS PINEDA MARÍA GUADALUPE**
Cargo:	ABOGADA AUXILIAR

Usuarios:	
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 52	**PARRA CALVO OLIVER DIDIERE**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR.

Usuarios:	
	• Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 53	**RODEA ALBAYTERO KAREN ANGÉLICA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no

Usuarios:	
	autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 54	**ARELLANO JUÁREZ LUCERO VIVIANA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 55	**HERNÁNDEZ ORTIZ MARÍA ANGÉLICA**
Cargo:	ABOGADA AUXILIAR

Usuarios:	
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 56	**FLORES MARTÍNEZ LAURA PATRICIA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR.

Usuarios:	
	• Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 57	**HERNÁNDEZ CRUZ NANCY LIZBETH**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no

Usuarios:	
	autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 58	**MALDONADO ROMERO JENNIFER NATALY**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 59	**VELÁZQUEZ JARAMILLO MAYVI DANIELA**
Cargo:	ABOGADA AUXILIAR

Usuarios:	
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 60	**SORIA HERNÁNDEZ LUIS ÁNGEL**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR.

Usuarios:	
	• Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 61	**SANDOVAL MEJÍA KARINA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no

Usuarios:	
	autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 62	**ZARAGOZÁ MORALES CYNTHIA ALEJANDRA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 63	**ÁLVAREZ OCHOA DANIEL ENRIQUE**
Cargo:	ABOGADO AUXILIAR

Usuarios:	
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 64	**ALVARADO DE LA CUESTA ANACLARA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR.

Usuarios:	
	• Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 65	**MUÑOZ MUÑOZ VERÓNICA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no

Usuarios:	
	autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 66	**RAMÍREZ DIAZ GRACIELA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 67	**VELÁZQUEZ DAZA LAURA ANABEL**
Cargo:	ABOGADA AUXILIAR

Usuarios:	
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 68	**JUÁREZ SANDOVAL FERNANDA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR.

Usuarios:	
	• Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 69	**REYES GÓMEZ LETICIA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no

Usuarios:	
	autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 70	**JÍMENEZ CLAVERIA LORENA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 71	**ANAYA VARGAS MARY JOSÉ**
Cargo:	ABOGADA AUXILIAR

Usuarios:	
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 72	**JUÁREZ GONZÁLEZ MÓNICA MARCELA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR.

Usuarios:	
	• Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 73	**CABALLERO MONTESINOS SANDRA GABRIELA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no

Usuarios:	
	autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 74	**CRUZ HERNÁNDEZ ADRIANA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 75	**PÉREZ LOZA MANUEL**
Cargo:	ABOGADO AUXILIAR

Usuarios:	
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 76	**RIVERO GONZÁLEZ ARACELI**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR.

Usuarios:	
	• Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 77	**VÁZQUEZ SANTIAGO GABRIELA**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos. • Implementar en su área las medidas necesarias a fin de evitar cualquier vulneración de datos personales. • Dar trámite a los asuntos que le sean asignados a través del SIGAR. • Realizar los proyectos de contestación a los asuntos asignados en el SIGAR. • Registrar en el SIGAR la conclusión de los asuntos.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de realizar transferencias no

Usuarios:	
	autorizadas de datos personales relativos a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 78	**CAPISTRÁN TOLENTINO MIGUEL ÁNGEL**
Cargo:	ASISTENTE DE PROCESOS
Funciones:	• Llevar el control y registro de entrada y salida de la documentación que debe integrarse al SIGAR. • Coadyuvar con el resguardo de forma segura de los expedientes y de la documentación recibida a través del SIGAR. • Acceder y consultar los documentos recibidos y que pudieran contener datos personales registrados en el SIGAR. • Accesar únicamente a los espacios físicos destinados para el resguardo de la documentación con especial cuidado, en el ámbito de su competencia, en los que contengan datos personales.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de transferir sin autorización los datos personales contenidos en los documentos relacionados a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 79	**DIAZ LOZANO ISHELL MONTSERRAT**
Cargo:	ASISTENTE DE PROCESOS

Usuarios:	
Funciones:	• Llevar el control y registro de entrada y salida de la documentación que debe integrarse al SIGAR. • Coadyuvar con el resguardo de forma segura de los expedientes y de la documentación recibida a través del SIGAR. • Acceder y consultar los documentos recibidos y que pudieran contener datos personales registrados en el SIGAR. • Accesar únicamente a los espacios físicos destinados para el resguardo de la documentación con especial cuidado, en el ámbito de su competencia, en los que contengan datos personales.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de transferir sin autorización los datos personales contenidos en los documentos relacionados a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 80	**GARAY ESCUTIA ARACELY**
Cargo:	ASISTENTE EJECUTIVO
Funciones:	• Integrar el registro de correspondencia. • Llevar el control y registro de entrada y salida de la documentación que debe integrarse al SIGAR. • Coadyuvar con el resguardo de forma segura de los expedientes y de la documentación recibida en el SIGAR. • Acceder y consultar los documentos recibidos y que pudieran contener datos personales registrados en el SIGAR.

Usuarios:	
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de transferir sin autorización los datos personales contenidos en los documentos relacionados a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 81	**OCHOA PÉREZ MARALY MONSERRAT**
Cargo:	ASISTENTE EJECUTIVO
Funciones:	• Integrar el registro de correspondencia. • Llevar el control y registro de entrada y salida de la documentación que debe integrarse al SIGAR. • Coadyuvar con el resguardo de forma segura de los expedientes y de la documentación recibida en el SIGAR. • Acceder y consultar los documentos recibidos y que pudieran contener datos personales registrados en el SIGAR.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de transferir sin autorización los datos personales contenidos en los documentos relacionados a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General.

Usuarios:	
	• Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 82	**ESTRADA GARCÍA LAURA**
Cargo:	ASISTENTE EJECUTIVO
Funciones:	• Integrar el registro de correspondencia. • Llevar el control y registro de entrada y salida de la documentación que debe integrarse al SIGAR. • Coadyuvar con el resguardo de forma segura de los expedientes y de la documentación recibida en el SIGAR. • Acceder y consultar los documentos recibidos y que pudieran contener datos personales registrados en el SIGAR.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de transferir sin autorización los datos personales contenidos en los documentos relacionados a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 83	**LEÓN FERIA EVELYN BERENICE**
Cargo:	ASISTENTE EJECUTIVO
Funciones:	• Integrar el registro de correspondencia. • Llevar el control y registro de entrada y salida de la documentación que debe integrarse al SIGAR. • Coadyuvar con el resguardo de forma segura de los expedientes y de la documentación recibida en el SIGAR.

Usuarios:	
	• Acceder y consultar los documentos recibidos y que pudieran contener datos personales registrados en el SIGAR.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de transferir sin autorización los datos personales contenidos en los documentos relacionados a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 84	**VILLARREAL PÉREZ SELENE BERENICE**
Cargo:	ASISTENTE EJECUTIVO
Funciones:	• Integrar el registro de correspondencia. • Llevar el control y registro de entrada y salida de la documentación que debe integrarse al SIGAR. • Coadyuvar con el resguardo de forma segura de los expedientes y de la documentación recibida en el SIGAR. • Acceder y consultar los documentos recibidos y que pudieran contener datos personales registrados en el SIGAR.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de transferir sin autorización los datos personales contenidos en los documentos relacionados a su encargo.

Usuarios:	
	• Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 85	**OLVERA CANCHOLA CLAUDIA**
Cargo:	ASISTENTE EJECUTIVO
Funciones:	• Integrar el registro de correspondencia. • Llevar el control y registro de entrada y salida de la documentación que debe integrarse al SIGAR. • Coadyuvar con el resguardo de forma segura de los expedientes y de la documentación recibida en el SIGAR. • Acceder y consultar los documentos recibidos y que pudieran contener datos personales registrados en el SIGAR.
Obligaciones:	• Mantener la integridad, disponibilidad y confidencialidad de la información. • Resguardar el acceso mediante el usuario y la contraseña que le sean asignados. • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la Dirección General. • Abstenerse de transferir sin autorización los datos personales contenidos en los documentos relacionados a su encargo. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.

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

Nombre del sistema	**SIGAR**
Tipo de soporte:	Físico y Electrónico
Descripción:	Soporte físico: Archivo donde están los documentos y/o expedientes. Soporte electrónico: Los datos del sistema se encuentran alojados en una base de datos administrada a través de un gestor y el SIGAR se encuentra en el equipo de cómputo de cada usuario, además de un respaldo en el servidor que almacena la base de datos.
Características del lugar donde se resguardan los soportes:	Soporte físico: Cuarto de archivo con ventilación natural, ventanas que permiten la entrada de luz, luminarias para luz artificial, puerta de acceso de madera y chapa de seguridad. Soporte electrónico: Alojamiento de los datos en un servidor ubicado en el cuarto de comunicaciones de la DGAJ.

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 77 a 89). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

3. ANÁLISIS DE RIESGOS.

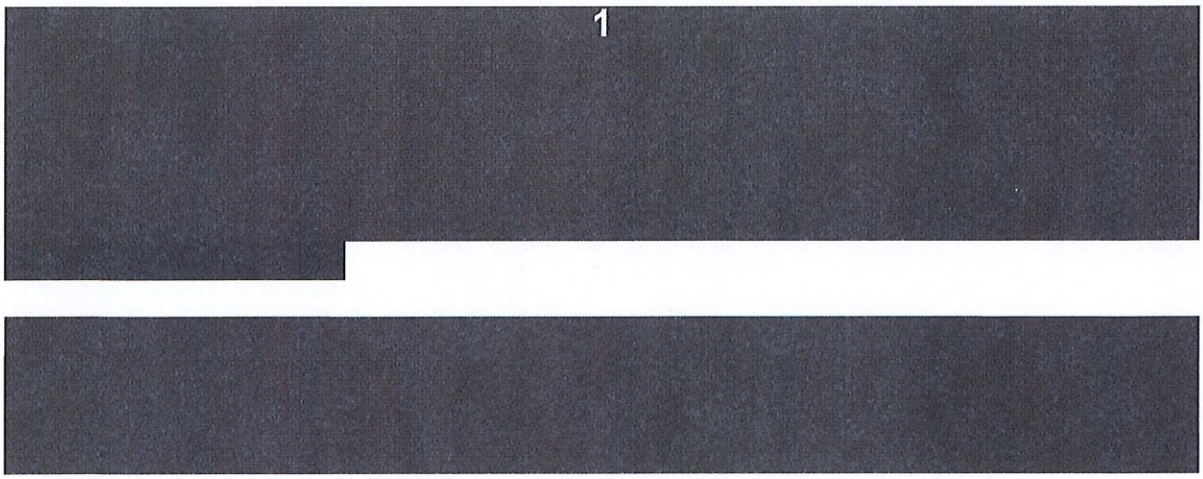
El proceso de análisis de riesgos debe considerar una evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño, además de contemplar la identificación de activos, estudio de causas y consecuencias de las amenazas y vulnerabilidades en el sistema de tratamiento de datos personales, permitiendo establecer parámetros para ponderar los efectos de posibles vulneraciones de seguridad.

Bajo estas consideraciones, la DGAJ en su análisis de riesgos, sigue una metodología basada en tres factores de riesgo que pudieran afectar de manera latente los datos personales tratados, consistentes en:

- Riesgo por tipo de dato. Determinado por el riesgo inherente del dato y el volumen de datos tratados.
- Riesgo por tipo de acceso. Se refiere al número de accesos potenciales a los datos personales.
- Riesgo por tipo de entorno. Se basa en el análisis del entorno desde el que se tiene acceso a los datos personales.

Ahora bien, debido a que el proceso de análisis requiere una evaluación cualitativa sobre la posibilidad de que un activo pueda sufrir alguna vulneración, esta DGAJ, para realizar el análisis del riesgo por tipo de dato, considerará realizar una clasificación de los datos personales tratados.

Para los efectos del presente análisis, los datos personales tratados por la DGAJ se clasificarán en cuatro categorías, de acuerdo con la criticidad de estos por nivel de riesgo inherente:



[redacted]

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 77 a 89). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 77 a 89). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR	
Riesgo	Impacto	Mitigación
1		

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 77 a 89). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR	
Riesgo	Impacto	Mitigación
1		

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 77 a 89). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR	
Riesgo	Impacto	Mitigación
1		

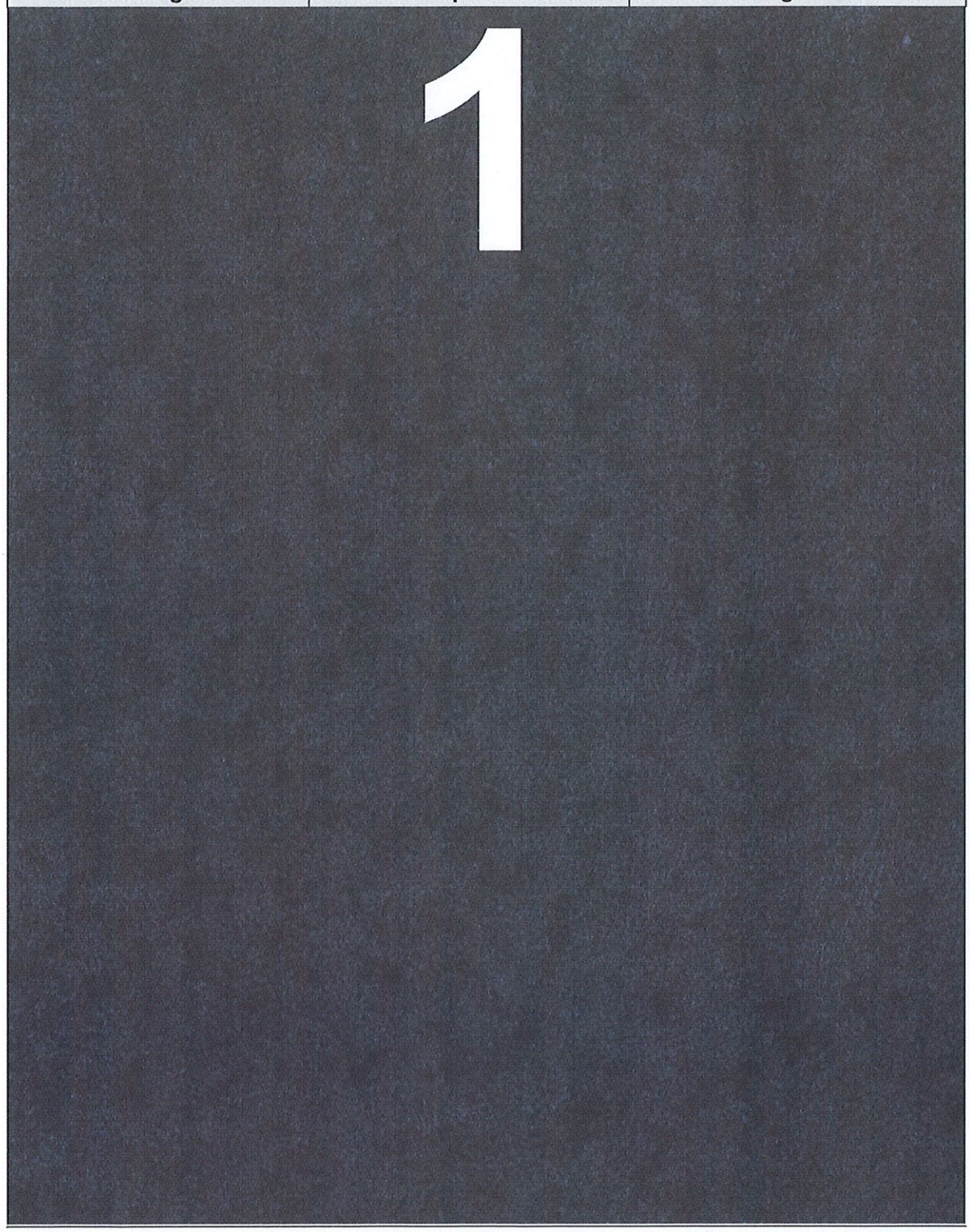
1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 77 a 89). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR	
Riesgo	Impacto	Mitigación
1		

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 77 a 89). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR	
Riesgo	Impacto	Mitigación
[redacted]		

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 77 a 89). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR	
Riesgo	Impacto	Mitigación
		

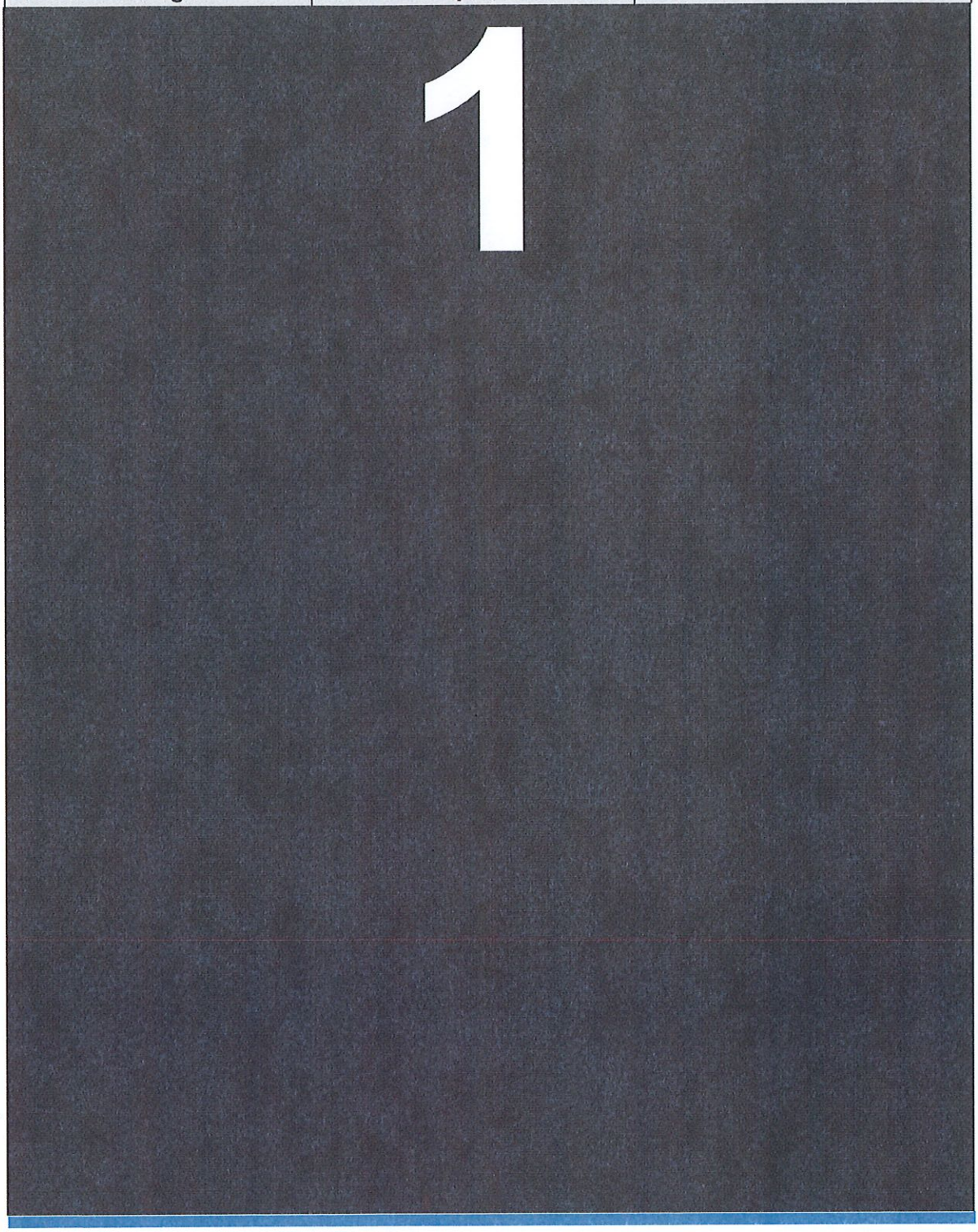
1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 77 a 89). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR	
Riesgo	Impacto	Mitigación
1		

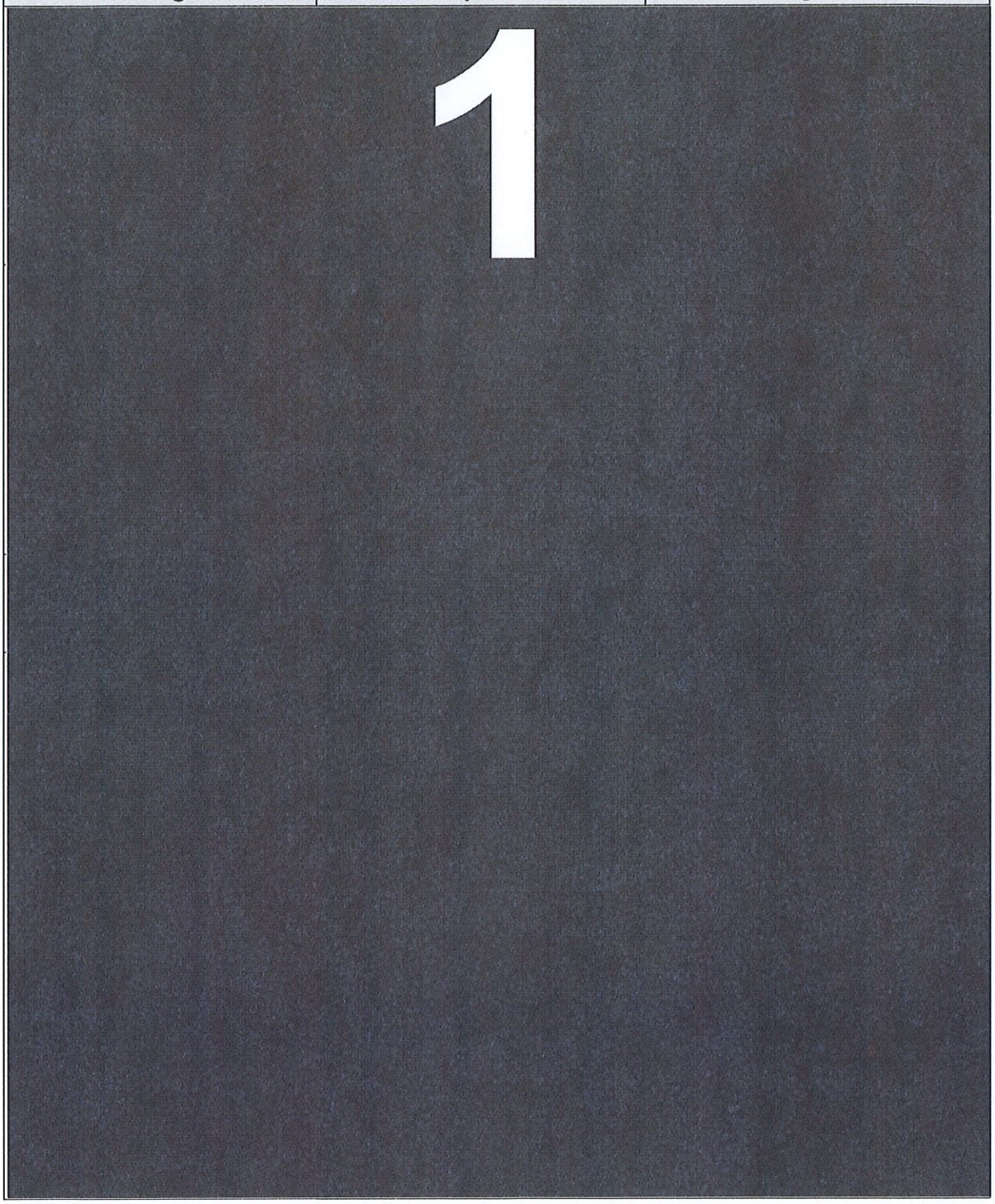
Nombre del sistema	SIGAR	
Riesgos Técnicos		
Riesgo	Impacto	Mitigación
1		

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 77 a 89). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

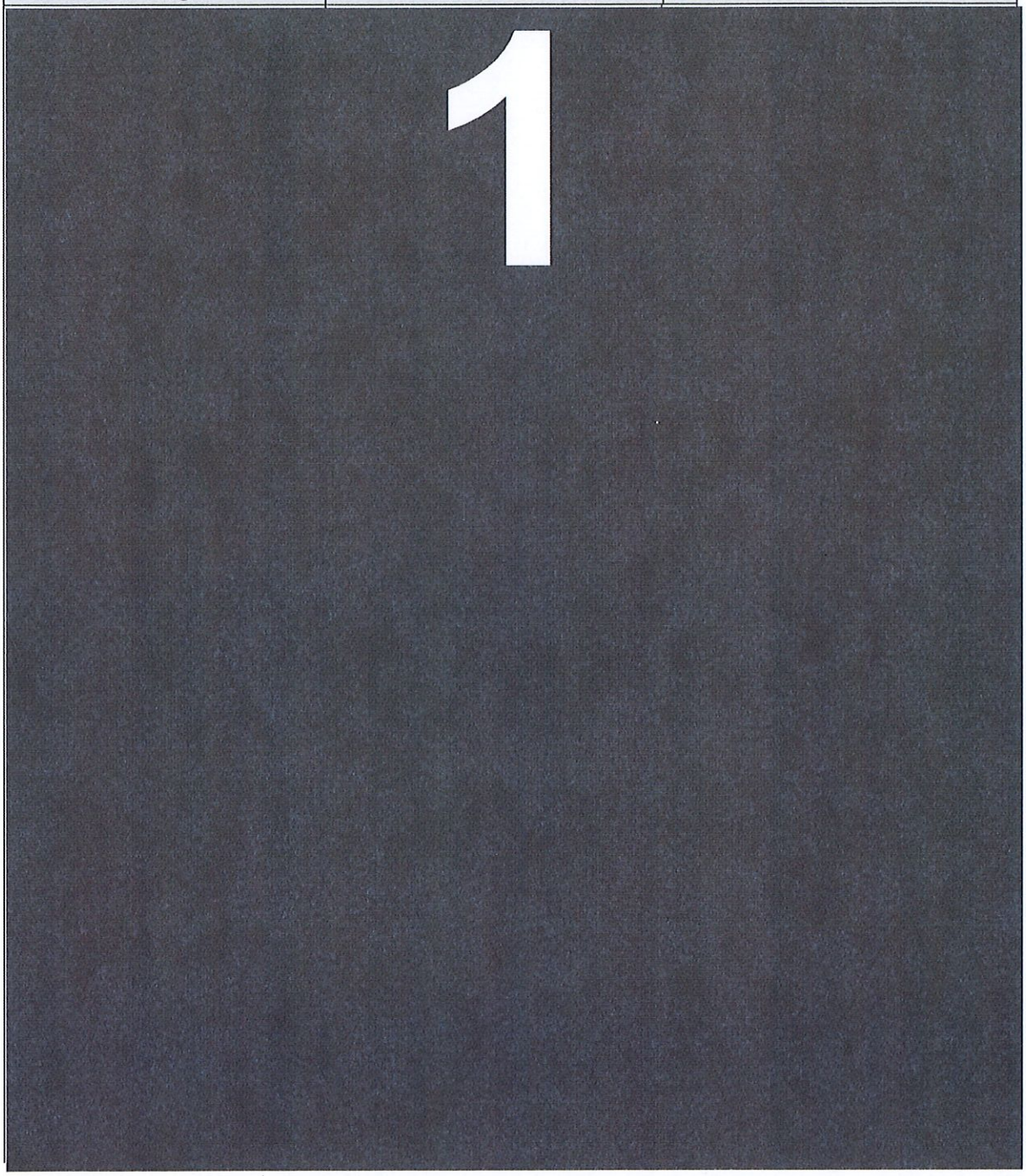
Nombre del sistema	SIGAR	
Riesgos Técnicos		
Riesgo	Impacto	Mitigación



1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 77 a 89). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

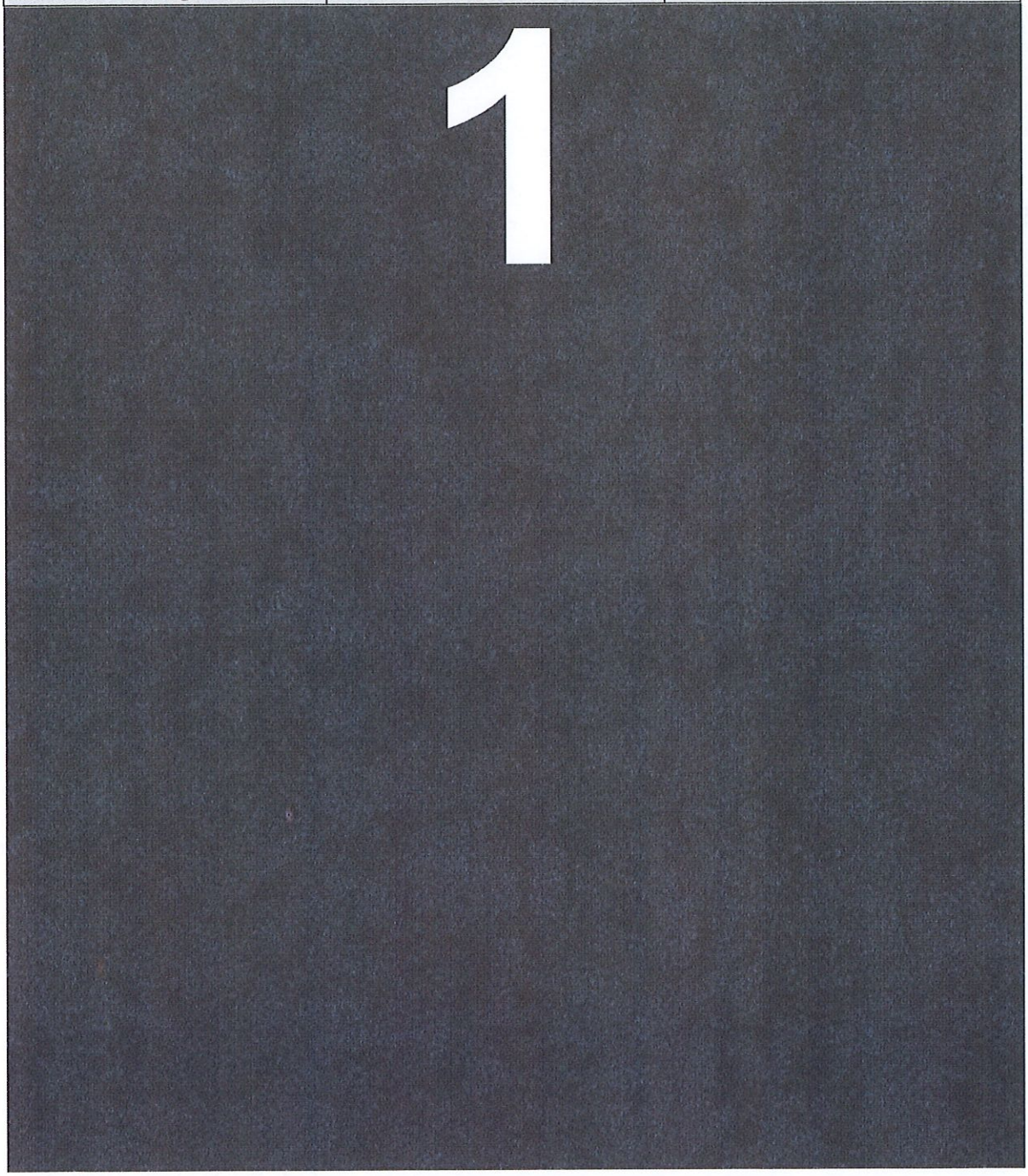
Nombre del sistema	SIGAR	
Riesgos Técnicos		
Riesgo	Impacto	Mitigación
		

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 77 a 89). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR	
Riesgos Técnicos		
Riesgo	Impacto	Mitigación
		

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 77 a 89). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR	
Riesgos administrativos y físicos		
Riesgo	Impacto	Mitigación



2. Texto eliminado: Apartado correspondiente a Análisis de Brecha (numeral 4, páginas 90 a 93). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

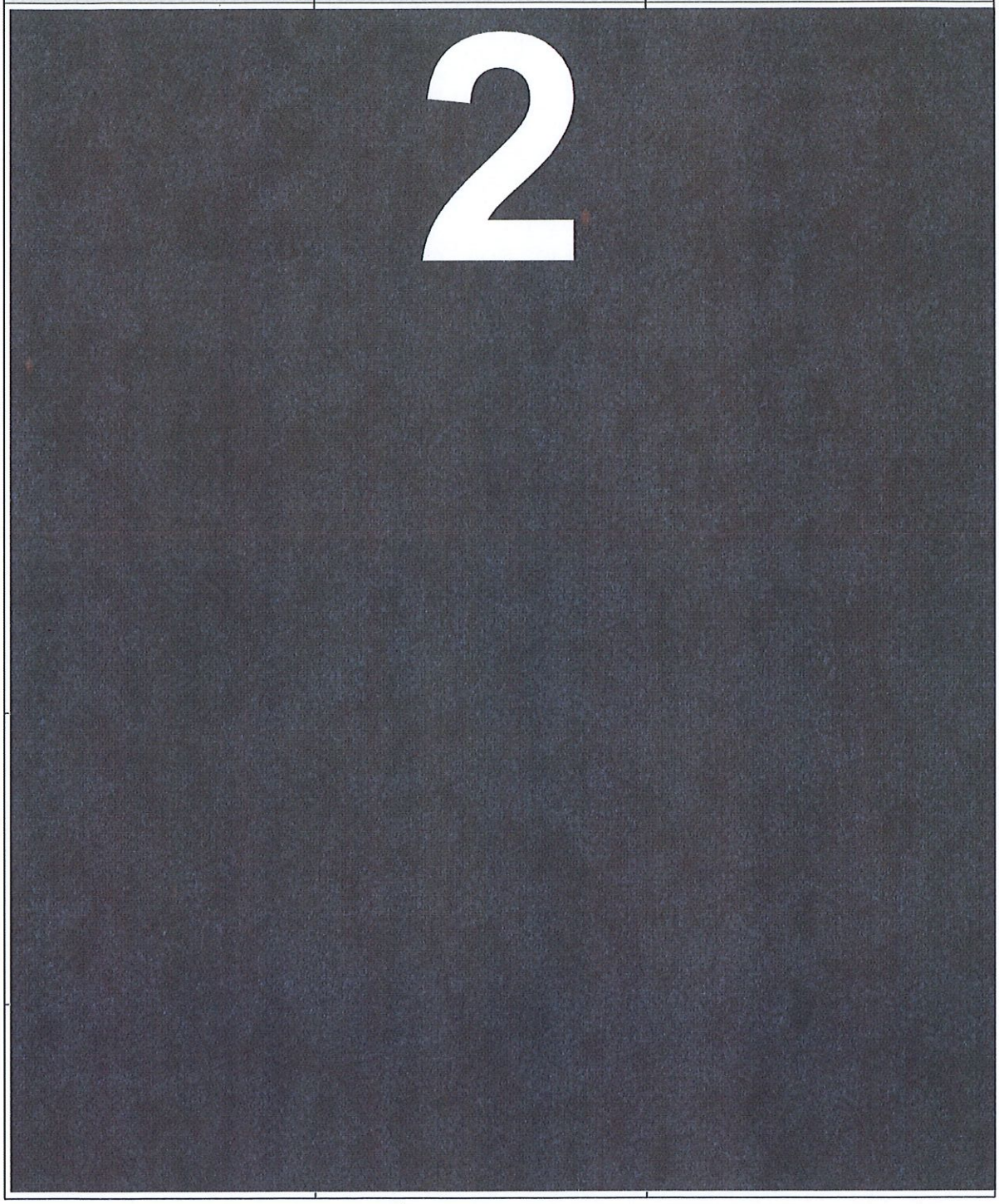
4. ANÁLISIS DE BRECHA.

De conformidad con la normatividad aplicable en materia de protección de datos personales, el análisis de brecha puede definirse como la concentración de elementos específicos que pueden existir entre las medidas de seguridad actuales y las medidas de seguridad deseables para alcanzar un nivel de protección adecuado para el tipo de activos que contienen los datos personales tratados, para ello es importante definir con claridad cuáles son las causas más relevantes que determinan la brecha (riesgos), identificar los indicadores y/o atributos de la situación actual (medidas de seguridad actuales) y elaborar un listado con la finalidad de medir o caracterizar la brecha (acciones para su remediación).

El presente análisis de brecha, pretende identificar la distancia que existe entre las medidas de seguridad implementadas en el tratamiento de los datos personales reportados y las necesarias, cuya información da sustento a los mecanismos institucionales en materia de protección de datos personales. Lo anterior con el objetivo de atenderlas de manera escalonada, para lo cual se deberá establecer un plan de trabajo.

Nombre del sistema	**SIGAR**	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
2		

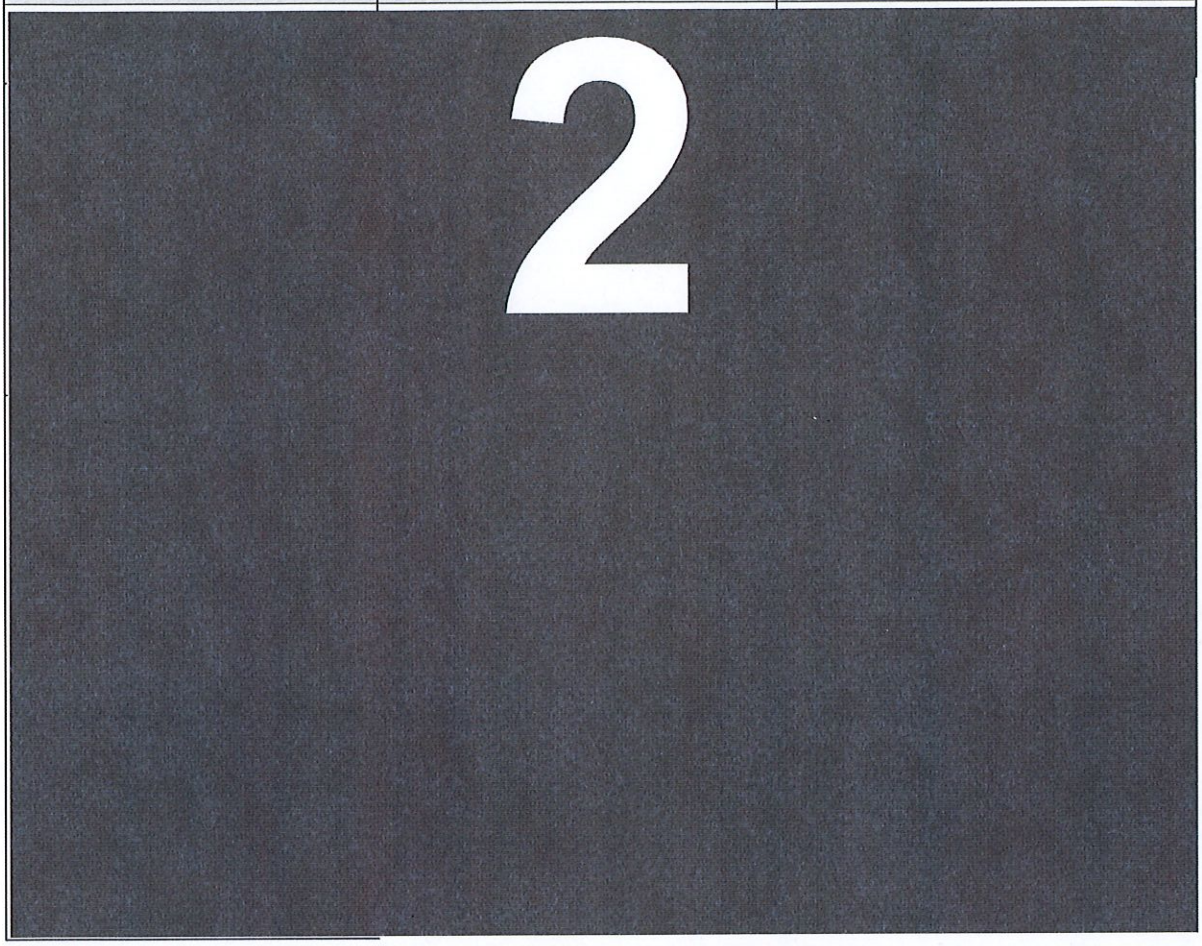
2. Texto eliminado: Apartado correspondiente a Análisis de Brecha (numeral 4, páginas 90 a 93). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
		

2. Texto eliminado: Apartado correspondiente a Análisis de Brecha (numeral 4, páginas 90 a 93). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR	
Medida de seguridad actual	Medida de seguridad necesaria	Acciones para remediación
2		

2. Texto eliminado: Apartado correspondiente a Análisis de Brecha (numeral 4, páginas 90 a 93). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
		

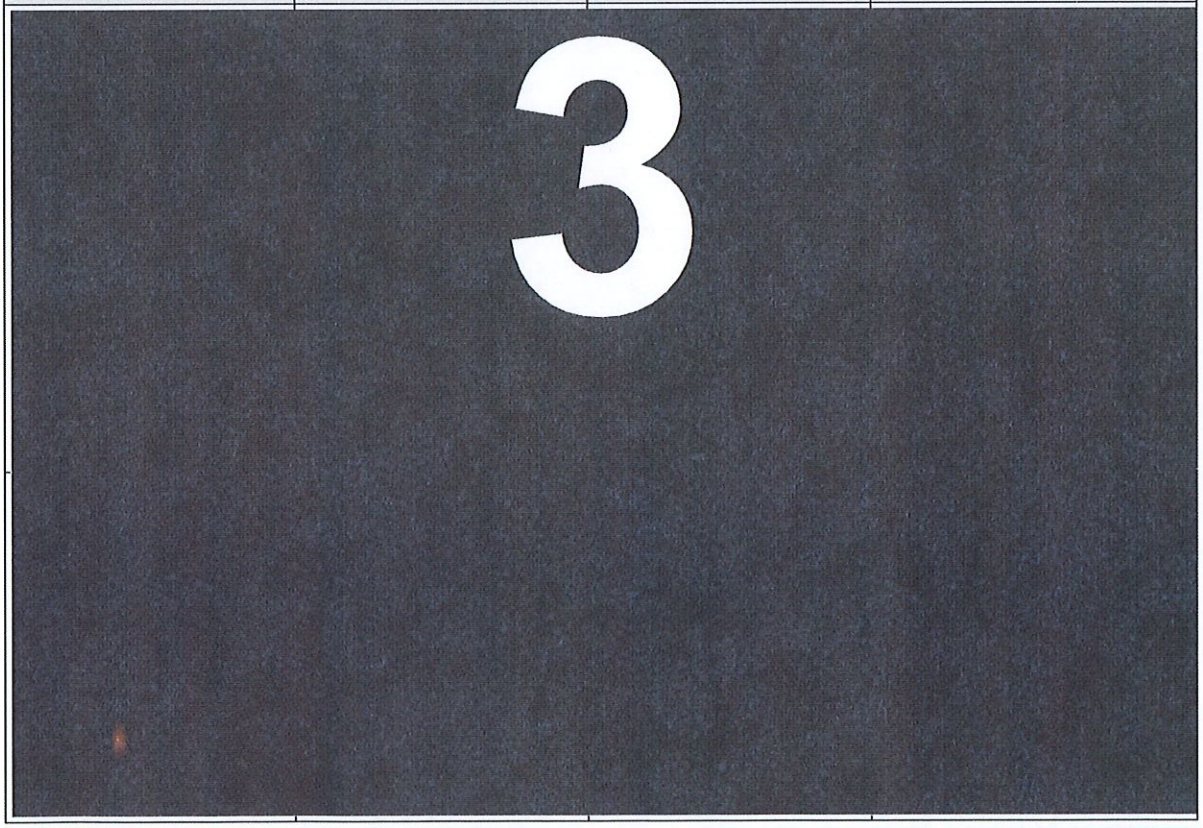
3. Texto eliminado: Apartado correspondiente a Plan de Trabajo (numeral 5, páginas 94 a 99). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

5. PLAN DE TRABAJO.

El presente plan de trabajo es un instrumento de planificación, entendiendo planificación como un proceso de concertación que, por su carácter dinámico, evoluciona y se adecua a un contexto, espacial y temporal.

La finalidad de este plan de trabajo será establecer la descripción y temporalidad de las acciones necesarias para la implementación de las medidas de seguridad faltantes, para el cumplimiento de las obligaciones normativas para la protección de los datos personales en su tratamiento.

Al definir las acciones mencionadas, se deberá priorizar las medidas de seguridad más relevantes e inmediatas a establecer, tomando en consideración los recursos designados; el personal interno y externo en la DGAJ, y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes. Lo anterior se vislumbra llevarlo a cabo de la siguiente forma:

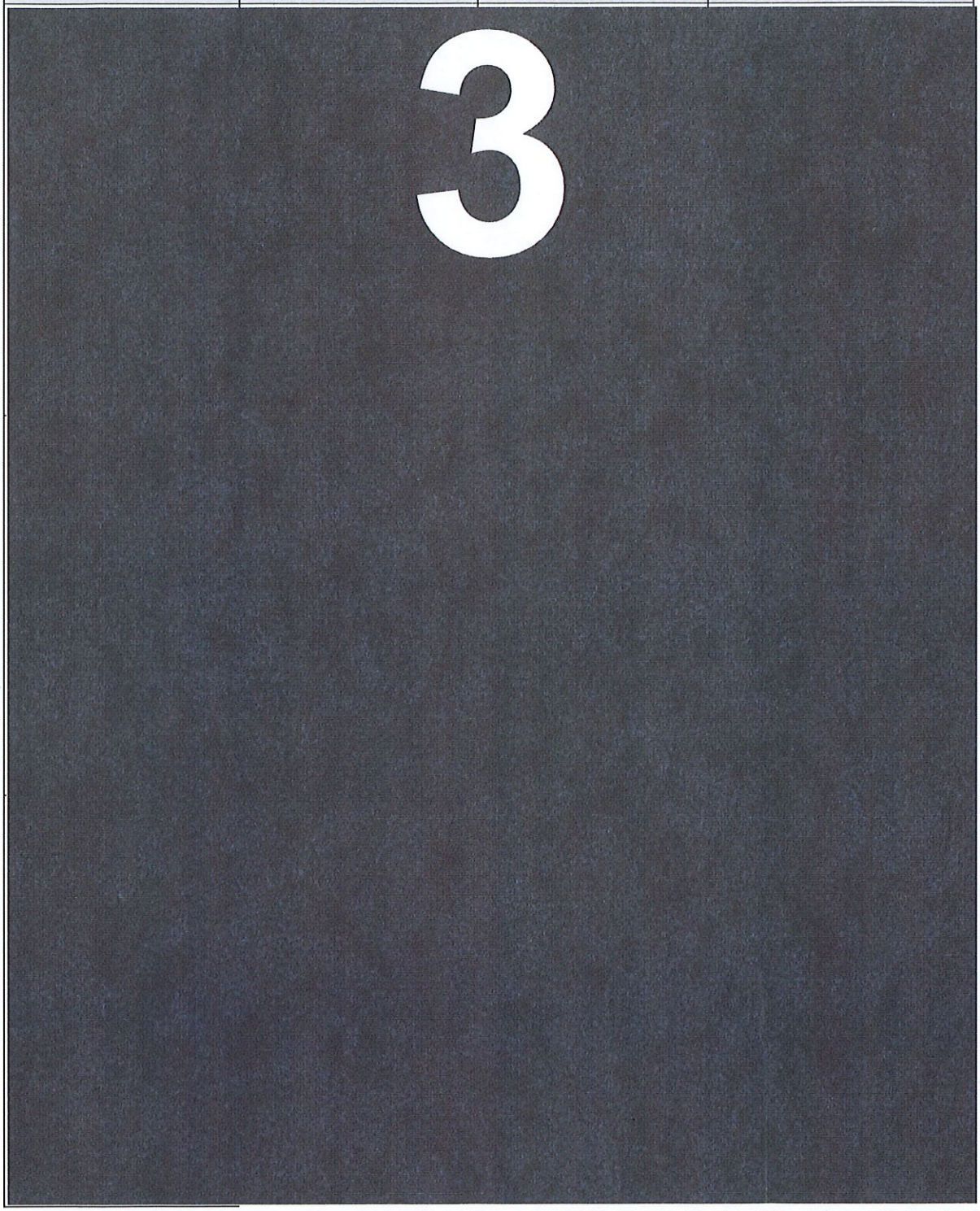
Nombre del sistema	**SIGAR**		
Actividad	**Descripción**	**Duración**	**Cobertura**
			

3. Texto eliminado: Apartado correspondiente a Plan de Trabajo (numeral 5, páginas 94 a 99). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR		
Actividad	Descripción	Duración	Cobertura
3			

3. Texto eliminado: Apartado correspondiente a Plan de Trabajo (numeral 5, páginas 94 a 99). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

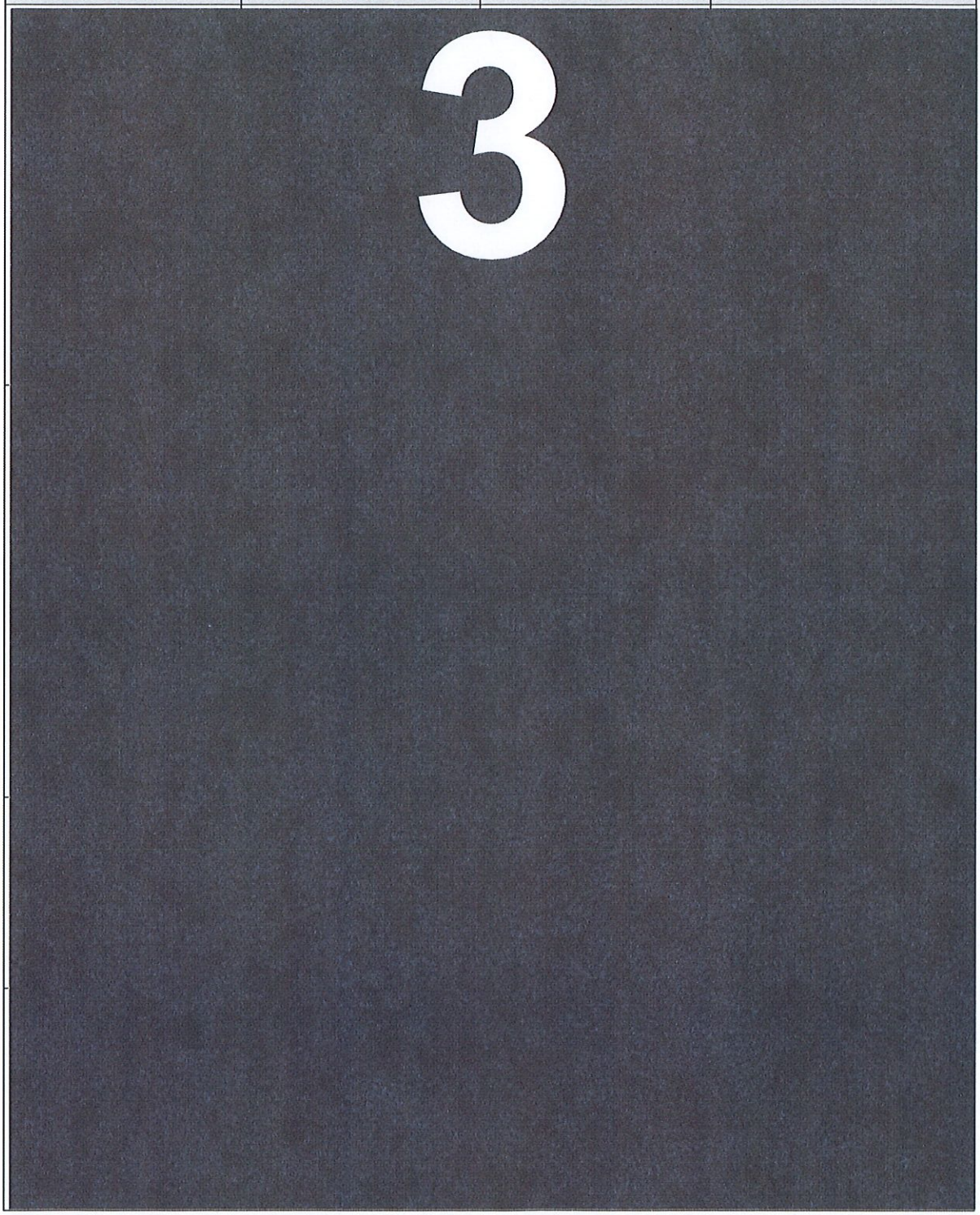
Nombre del sistema	SIGAR		
Actividad	Descripción	Duración	Cobertura



3. Texto eliminado: Apartado correspondiente a Plan de Trabajo (numeral 5, páginas 94 a 99). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR		
Actividad	Descripción	Duración	Cobertura
3			

3. Texto eliminado: Apartado correspondiente a Plan de Trabajo (numeral 5, páginas 94 a 99). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR		
Actividad	Descripción	Duración	Cobertura
			

3. Texto eliminado: Apartado correspondiente a Plan de Trabajo (numeral 5, páginas 94 a 99). Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

Nombre del sistema	SIGAR		
Actividad	Descripción	Duración	Cobertura
3			

4. Texto eliminado: Apartado correspondiente a Medidas de Seguridad (numeral 6, fracción I, páginas 100 y 101, fracción III, numerales 1, 2, 3, 4, 5 y 6 páginas 102 y 103, fracción IV, numeral 3, cuatro líneas de la página 104, fracción V, numeral 2, página 105, fracciones VII, VIII y IX, página 106).
Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS.

I. TRANSFERENCIAS DE DATOS PERSONALES.

Nombre del sistema:	SIGAR
4	

Nombre del sistema:	SIGAR
[redacted]	[redacted] 4

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

1. Dentro de las Medidas de seguridad implementadas para el resguardo de los soportes físicos del sistema, de manera que se evite la alteración, pérdida o acceso no autorizado a los datos personales que obran en el archivo, se encuentran, entre otras:

- Distribución de responsabilidades.
- Sistema de monitoreo, en relación con el turno de cada asunto.
- Control de entrada física para el personal de la DGAJ.
- Seguridad en entornos de trabajo.
- Puertas con cerradura reforzada.
- Gabinetes de seguridad.
- Seguridad en el cableado de las instalaciones de la DGAJ.
- Sistema de cámaras de videovigilancia.
- Condiciones climáticas mínimas requeridas para el resguardo de los expedientes físicos.
- Ambiente limpio, seco y ventilado, sin intercambio constante de aire.
- Control de biota nociva.
- Espacio de resguardo adecuado.
- Se ubica en un lugar sin riesgos de humedad subterránea, sin problemas de inundación y estable.
- Se cuenta con un área suficiente para albergar la documentación actual.
- Mobiliario de resguardo adecuado para las unidades de archivo que albergan los activos de la información, el cual cuenta con el diseño acorde con la dimensión de las unidades de archivo, se evita que los bordes o aristas produzcan daños sobre los documentos.

4. Texto eliminado: Apartado correspondiente a Medidas de Seguridad (numeral 6, fracción I, páginas 100 y 101, fracción III, numerales 1, 2, 3, 4, 5 y 6 páginas 102 y 103, fracción IV, numeral 3, cuatro líneas de la página 104, fracción V, numeral 2, página 105, fracciones VII, VIII y IX, página 106).
Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

4. Texto eliminado: Apartado correspondiente a Medidas de Seguridad (numeral 6, fracción I, páginas 100 y 101, fracción III, numerales 1, 2, 3, 4, 5 y 6 páginas 102 y 103, fracción IV, numeral 3, cuatro líneas de la página 104, fracción V, numeral 2, página 105, fracciones VII, VIII y IX, página 106).
Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

- La estantería y/o gavetas están fabricadas con láminas metálicas sólidas, resistentes y estables.
- Las cajas de archivo no se encuentran saturadas.
- Los expedientes están organizados atendiendo lo dispuesto en la normatividad de archivos de la Universidad.
- Se evitan cajas semivacías y los expedientes se guardan de forma ordenada siguiendo un orden ascendente y cronológico en cajas correlativas, según un orden de mayor a menor.
- Para el resguardo de los soportes físicos del sistema se emplean folders resistentes, lo cuales son foliados conforme al código de clasificación correspondiente, de acuerdo a los Lineamientos de Control y Consulta archivística vigentes.

2. Las personas que tienen acceso a los soportes físicos del sistema, así como al archivo, quedaron señaladas en el apartado 4, "Del Inventario de Sistemas de Tratamiento de Datos Personales".

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA.

[redacted]

4. Texto eliminado: Apartado correspondiente a Medidas de Seguridad (numeral 6, fracción I, páginas 100 y 101, fracción III, numerales 1, 2, 3, 4, 5 y 6 páginas 102 y 103, fracción IV, numeral 3, cuatro líneas de la página 104, fracción V, numeral 2, página 105, fracciones VII, VIII y IX, página 106).
Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

4 [redacted]

IV. REGISTRO DE INCIDENTES.

El procedimiento de atención de incidentes que se tiene implementado es el siguiente:

a) El director o jefe de departamento, según corresponda, elabora y entrega un informe al responsable de datos personales a más tardar al día siguiente de haber ocurrido el incidente. Dicho informe precisa los soportes físicos y, en su caso, electrónicos comprometidos y cuando corresponda los recuperados.

b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Su integridad se garantiza generando y almacenando un resumen creado y respaldándola en un CD-R después de registrar un incidente.

c) En caso de robo o extravío de datos personales, el responsable del sistema de tratamiento de datos personales, al tener conocimiento del incidente, da vista al titular de la dependencia para su conocimiento y al titular del área jurídica o aquél que tenga facultades para presentar denuncias o querellas ante el Ministerio Público para que, en el ámbito de sus atribuciones, determine lo conducente.

4. Texto eliminado: Apartado correspondiente a Medidas de Seguridad (numeral 6, fracción I, páginas 100 y 101, fracción III, numerales 1, 2, 3, 4, 5 y 6 páginas 102 y 103, fracción IV, numeral 3, cuatro líneas de la página 104, fracción V, numeral 2, página 105, fracciones VII, VIII y IX, página 106).
Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

d) En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el responsable del sistema de tratamiento de datos personales da aviso por escrito a dichos titulares, a más tardar a los 3 días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Adicionalmente, se da aviso por correo electrónico o por teléfono.

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, etc.

2. El registro está en soporte físico y en soporte electrónico.

4 [redacted]

4. Para el caso de soportes electrónicos, quien autoriza la recuperación de datos es el administrador del sistema.

V. ACCESO A LAS INSTALACIONES.

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

Para el control de acceso a la DGAJ, se cuenta con un punto de acceso mediante control biométrico, para el personal del área, operado por el Departamento de Informática, de igual manera se cuenta con un sistema de cámaras de videovigilancia.

Para las personas que acceden a las instalaciones:

a) Se identifican:

- Personas que laboran en la DGAJ mediante el reconocimiento de la huella dactilar.

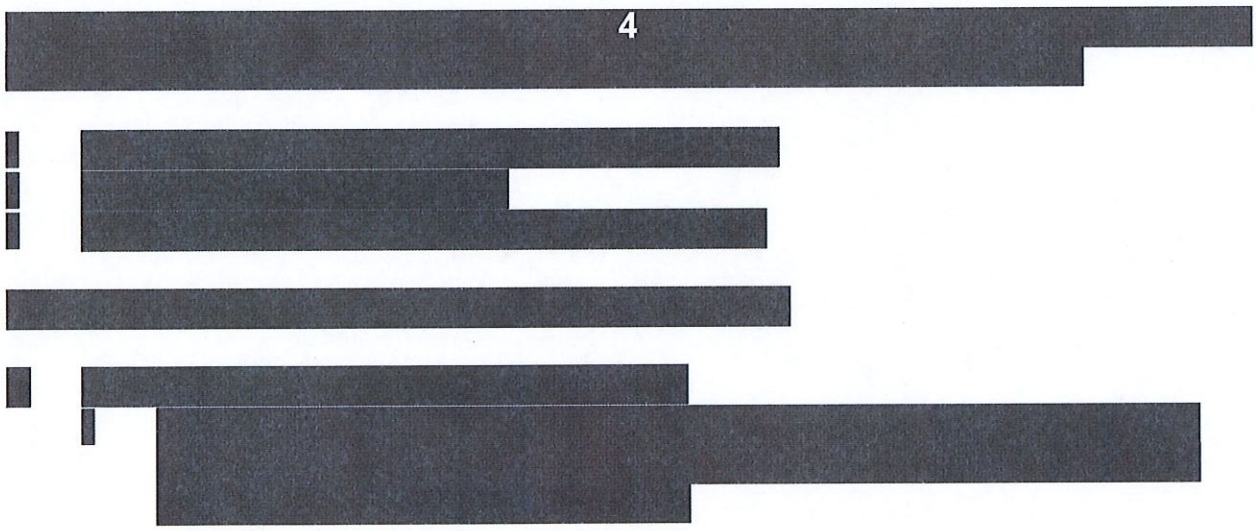
4. Texto eliminado: Apartado correspondiente a Medidas de Seguridad (numeral 6, fracción I, páginas 100 y 101, fracción III, numerales 1, 2, 3, 4, 5 y 6 páginas 102 y 103, fracción IV, numeral 3, cuatro líneas de la página 104, fracción V, numeral 2, página 105, fracciones VII, VIII y IX, página 106).
Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

- Personas externas a la DGAJ: el personal adscrito a la DGAJ corrobora su identidad y el motivo de su visita.

b) Se autentifican:
- Personas que laboran en la DGAJ: con el mecanismo enunciado en el inciso a), comparando los datos con los almacenados en la base de datos de control de acceso.
- Personas externas a la DGAJ: con algún documento de identificación que demuestre su identidad.

c) Se autoriza el acceso, de acuerdo a:
- Personas que laboran en la DGAJ: Automáticamente, después de corroborar su identidad y autentificarla.
- Personas externas a la DGAJ: después de corroborar su identidad y autentificarla.

2. Seguridad perimetral interior donde se ubica el sistema físico y electrónico.



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

Derivado del objetivo del sistema no se requiere la actualización de la información relacionada con los datos personales que obran en el mismo.

VII. PERFILES DE USUARIO Y CONTRASEÑAS.

[redacted]

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS.

[redacted]

IX. PLAN DE CONTINGENCIA.

[redacted]

4. Texto eliminado: Apartado correspondiente a Medidas de Seguridad (numeral 6, fracción I, páginas 100 y 101, fracción III, numerales 1, 2, 3, 4, 5 y 6 páginas 102 y 103, fracción IV, numeral 3, cuatro líneas de la página 104, fracción V, numeral 2, página 105, fracciones VII, VIII y IX, página 106).
Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.

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

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

Nombre del sistema	SIGAR	
Recurso	**Descripción**	**Control**
Revisión Interna	Actividad enfocada al examen, sistemático y de evaluación a las medidas físicas y administrativas realizadas de seguridad; con el propósito de determinar el grado de eficacia, eficiencia, efectividad, y apego a la normatividad con que se han implementado en cada una de estas medidas de seguridad	El trabajo de auditoría comprende tres etapas: Planeación, Ejecución y Emisión del Informe. Por lo tanto, el control de la revisión interna, se lleva a cabo primordialmente con el Cronograma de Actividades a Desarrollar, se detallan las actividades que el grupo de revisión efectuará desde el inicio hasta su conclusión.
Revisión aleatoria	Actividad enfocada al examen a las medidas físicas de seguridad; con el propósito de determinar el grado de eficacia, eficiencia, efectividad, con que se han implementado en el resguardo del SIGAR de la DGAJ.	El control de la actividad se da a través de la creación de una muestra aleatoria de filas a partir de una o más columnas que contengan las medidas físicas de seguridad. De esta manera se genera una muestra con los resultados obtenidos de la revisión correspondiente.
Prueba de penetración	La prueba de penetración física, es la actividad encaminada a obtener evidencia, respecto del posible acceso que se pudiera tener al sistema de datos personales, para lo cual, entre otras actividades se llevan a cabo: Capturar evidencia fotográfica del acceso a	El control de la actividad se presenta a través de un listado con las observaciones y posibles vulneraciones en las medidas físicas de seguridad del sistema de datos personales.

Nombre del sistema	SIGAR	
Recurso	Descripción	Control
	áreas restringidas. Estudio de las instalaciones para detectar puntos a explorar y posibles vulneraciones.	

7.2. Procedimiento para la revisión de las medidas de seguridad.

Está relacionado con el apartado anterior.

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

No aplica, toda vez que no se han realizado evaluaciones.

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

No aplica, toda vez que no se han realizado evaluaciones.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN.

Justificación

Uno de los principales compromisos de la Universidad es dar cumplimiento a la normatividad en materia de protección de datos personales, ya que impacta de manera directa en las funciones sustantivas de la misma, por ello, se considera que la sensibilización y capacitación permanente del personal que integra la DGAJ resulta de vital importancia.

Por ello, esta DGAJ considera importante generar esquemas de trabajo interdependientes con la Unidad de Transparencia de la UNAM para la protección de los datos personales que posee.

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

En ese sentido, se presenta anexo al presente el Programa Universitario de Capacitación en Protección de Datos Personales 2022, propuesto por la Unidad de Transparencia y aprobado por el Comité de Transparencia de esta Universidad en su sesión de 12 de agosto de 2022, del cual participa el personal de esta área cuyas funciones derivan en el tratamiento de datos personales y forma parte integral del presente documento.

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

La difusión de la protección a los datos personales que da esta DGAJ, se realiza a través de los avisos de privacidad tanto integral como simplificado, por los cuales se hace del conocimiento de los interesados, el tratamiento y finalidades que se da a los datos personales.

9. MEJORA CONTINUA.

9.1. Actualización y mantenimiento de sistemas de información.

Dada la operatividad y funcionamiento del SIGAR en el presente año no se contempla ninguna actualización al sistema referido.

9.2. Actualización y mantenimiento de equipo de cómputo.

Nombre del sistema	**SIGAR**		
Actividad	**Descripción**	**Duración**	**Cobertura**
Actualización de software	Los equipos están configurados para recibir de forma automática las actualizaciones de software y son instaladas de acuerdo a las horas activas del equipo, aunado a esto, el Departamento de Informática realiza búsquedas manuales y periódica de ellas.	Actividad permanente	El 100% de los equipos de cómputo de la DGAJ
Mantenimiento	Los servicios se realizan anualmente. El personal del Departamento de Informática realiza una revisión interna del CPU y se determina si el mantenimiento es preventivo o correctivo. La fecha de mantenimiento se coordina con el área y se determina el momento adecuado para realizarlo.	3 días	El 100% de los equipos de cómputo de la DGAJ

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

Nombre del sistema	SIGAR	
Proceso	**Descripción**	**Responsable**
Respaldos de la base de datos	Se realizan respaldos con periodicidad variable o cada que la Dirección General solicita un corte del avance hasta la fecha.	Departamento de Informática, ejecución máxima de 2 días hábiles.

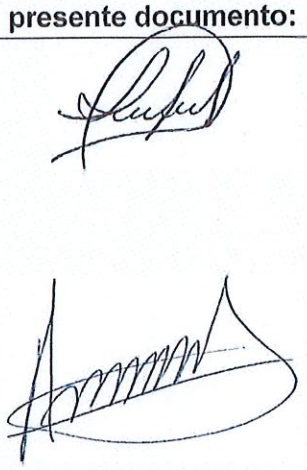
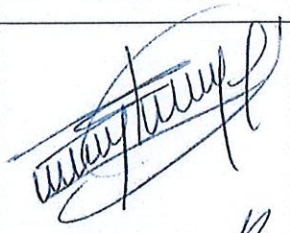
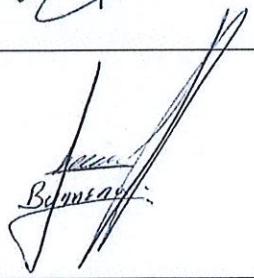
9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos.

Nombre del sistema	SIGAR	
Proceso	**Descripción**	**Responsable**
Borrado seguro previa baja del equipo	Se realiza un proceso de borrado parcial de la información a través de la línea de comandos o de forma total con ayuda de un software especializado, posteriormente se llena la responsiva de borrado de información y se entrega el equipo en el almacén de bajas.	El borrado de información y llenado de la responsiva corre a cargo del Departamento de Informática y la entrega del equipo en almacén es apoyada por el Departamento de Bienes y Suministros. El proceso completo conlleva una duración máxima de 5 días hábiles.

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

Debido a la relevancia del sistema de tratamiento de datos personales SIGAR, se considera improcedente contar con un procedimiento de cancelación del mismo, por el momento.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD.

		Nombre y firma de quienes revisaron el presente documento:
Responsables del desarrollo:	Lic. Lizbeth Betzai Martínez Muñoz, Coordinadora de Gestión de la DGAJ teléfono: 55562 32300, extensión: 26327, correo electrónico: dgaj@unam.mx Ing. Armando Vázquez Díaz, Jefe del Departamento de Informática, de la DGAJ teléfono: 55562 32300, extensión: 48049, correo electrónico: dinformatica.dgaj@unam.mx	
Revisó:	Mtra. Mary Triny Pérez Olivares, Secretaria de Planeación, teléfono: 55562 32300, extensión: 48060, correo electrónico: splaneacion.dgaj@unam.mx	
Autorizó:	Lic. Jorge Barrera Gutiérrez, Director General de Asuntos Jurídicos, teléfono: 55562 32300, extensión: 48080, correo electrónico: jbarrera@unam.mx	
Fecha de aprobación:	12 de agosto de 2022	

Partes clasificadas: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 77 a 89), Análisis de Brecha (numeral 4, páginas 90 a 93), Plan de Trabajo (numeral 5, páginas 94 a 99) y Medidas de Seguridad (numeral 6, fracción I, páginas 100 y 101, fracción III, numerales 1, 2, 3, 4, 5 y 6 páginas 102 y 103, fracción IV, numeral 3, cuatro líneas de la página 104, fracción V, numeral 2, página 105, fracciones VII, VIII y IX, página 106).
Fundamento legal y motivación: Artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de tratarse de información que permitiría obstruir la prevención de delitos.
Fecha y número de acta de la sesión: 11ª sesión extraordinaria del 24/08/2022 y CTUNAM/529/2022.

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/529/2022

Visto el expediente relativo a la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública, que someten la **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado** y la **Dirección General de Asuntos Jurídicos,** en relación con sus respectivos **Documentos de Seguridad**, se procede a dictar la presente resolución con base en los siguientes:

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

I. Con fecha 26 de enero de 2017 se publicó en el Diario Oficial de la Federación el Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.

II. Mediante Acuerdo **ACT-PUB/19/12/2017.10**, de fecha 19 de diciembre de 2017, publicado en el Diario Oficial de la Federación con fecha 26 de enero de 2018, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

III. A través del Acuerdo **ACT-PUB/11/11/2020.05**, de fecha 11 de noviembre de 2020, publicado en el Diario Oficial de la Federación con fecha 25 de noviembre de 2020, dicho Órgano Garante aprobó la adición de un Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público, a fin de establecer las disposiciones generales que permitirán desarrollar el procedimiento de diseño y aplicación del sistema y procedimiento para llevar a cabo la evaluación sobre el desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia.

IV. Por Acuerdo **ACT-PUB/17/11/2021.05**, de fecha 17 de noviembre de 2021, publicado en el Diario Oficial de la Federación con fecha 26 de noviembre de 2021, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los "Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados".

V. Los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público, así como las reglas Décima Tercera y Décima Cuarta del apartado "V. Reglas de Generales de Evaluación" del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establecen que la información y documentos que se pongan a disposición de los titulares de datos personales y del Instituto, deberán ser revisados por el responsable a fin de verificar que no contengan información confidencial o reservada y, de ser el caso, deberá publicarse la versión pública de dicha documentación.

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

VI. En términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 34, fracción II del Reglamento de Transparencia y Acceso a la Información Púbica de la Universidad Nacional Autónoma de México, la clasificación de la información será procedente cuando, entre otros supuestos, se determiné mediante una resolución de autoridad competente.

VII. Mediante oficio **CSAMorelos/533.01/0289/2022**, recibido fecha 18 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Coordinación de Servicios Administrativos Morelos,** informó lo siguiente:

> *"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[1]; exige elaborar versión pública del documento de seguridad de esta área universitaria.*
>
> *Una vez analizada la información que se solicitó en el primer punto del 'Documento de seguridad', se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.*

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

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

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

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*16 -40*
b) Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*16 -40*
c) Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*16 -40*

Los fundamentos y motivos se exponen a continuación:

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

- *Divulgar el análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

- *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

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

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de

diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

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

VIII. Mediante oficio **CVTT/038/2022**, recibido fecha 18 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Coordinación de Vinculación y Transferencia Tecnológica** informó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[2]; exige elaborar versión pública del documento de seguridad de esta área universitaria.

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

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

técnica, administrativa y física de los datos personales que los titulares confían a esta institución.

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

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

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
Anexo 1. Inventario de sistemas de tratamiento de datos personales	*El inventario de los sistemas de tratamiento de datos personales contiene información sobre las rutas de acceso a soportes digitales de la información y cuentas, los cuales pueden ser utilizados para un ataque informático a los activos críticos y no críticos.*	*12-95*
Anexo 2. Estructura y descripción de los sistemas de tratamiento de datos personales	*La estructura y descripción de los sistemas de tratamiento de datos personales contiene información sobre las rutas y métodos de acceso a soportes digitales y físicos de la información, los cuales pueden ser utilizados para un ataque a los activos críticos y no críticos.*	*97-128*
Anexo 3. Diagramas de arquitectura	*Los diagramas de arquitectura de los soportes digitales contienen el flujo de información entre los componentes, sus rutas de acceso a soportes digitales y describe las medidas de seguridad implementadas, información que puede ser utilizada para un ataque informático a los activos críticos y no críticos.*	*130-156*

Anexo 5. Análisis de riesgos y análisis de brecha	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.* *El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*270-381*
Anexo 6. Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*383-389*

Los fundamentos y motivos se exponen a continuación:

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

- *Divulgar el inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia evidencian los nuevos*

controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.

- *En este sentido la revelación de la información que obra el inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, el análisis de riesgo, el análisis de brecha, las políticas de respaldo y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

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

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

En tal sentido, proteger la información de los documentos relativos al inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad porque se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a

que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

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

IX. Mediante oficio **ET/DGTIC/040/2022**, recibido con fecha 19 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General de Cómputo y Tecnologías de Información y Comunicación** informó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[3]; exige elaborar versión pública del documento de seguridad de esta área universitaria.

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

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

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

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

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

Reserva total o parcial	***Anexos o Políticas***	***Contenido y su afectación***	***Páginas***
Reserva Parcial	***a)*** *Inventario de datos personales*	*El inventario contiene información técnica y operativa que permite identificar los espacios físicos e infraestructura tecnológica en que se resguardan datos personales*	*19 de 47*
Reserva Total	***b)*** *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*63*
Reserva Total	***c)*** *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*20*
Reserva Total	***d)*** *Plan de Trabajo y Medidas de Seguridad.*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*1*
Reserva	***e)*** *Política de*	*Las políticas contienen información*	*4*

Total	*autenticación y control de acceso*	*del conjunto de reglas diseñadas para determinar a quién se le concede acceso a un lugar restringido o a una información restringida relacionada con los datos personales en posesión de la dependencia.*	
Reserva Total	***f)** Política de seguridad física y ambiental*	*Las políticas contienen información sobre las medidas que se adoptarán para proteger los sistemas, los edificios y la infraestructura de apoyo de los sistemas de datos personales contra las amenazas asociadas con ambiente físico.*	*4*

Los fundamentos y motivos se exponen a continuación:

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

- *Divulgar el inventario de datos personales, análisis de riesgo, el análisis de brecha, las políticas de autenticación y control de acceso, así como de seguridad física y ambiental y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planemos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

- *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha … y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

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

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

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

Por tales motivos, respetuosamente, se propone la reserva parcial del inventario de datos personales, y la reserva total del análisis de riesgo, el análisis de brecha, las políticas de autenticación y control de acceso, así como de Seguridad física y ambiental y el plan de trabajo cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta dependencia universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento

de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

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

X. Mediante oficio **DGRU/DG/090/2022/am** recibido con fecha 19 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General de Repositorios Universitarios** informó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[4]; exige elaborar versión pública del documento de seguridad de esta área universitaria.

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

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

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

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

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*Anexo 1. 38-44* *Anexo 2. 91-101* *Anexo 3. 154-163* *Anexo 4. 201-210* *Anexo 5. 254-266* *Anexo 6. 317-329* *Anexo 7. 377-393* *Anexo 8. 437-457* *Anexo 9. 514-529* *Anexo 10. 579-586*
b) *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*Anexo 1. 45-48* *Anexo 2. 101-106* *Anexo 3. 163-165* *Anexo 4. 210-214* *Anexo 5. 266-270* *Anexo 6. 329-332* *Anexo 7. 393-398* *Anexo 8. 457-462* *Anexo 9. 529-533* *Anexo 10. 586-589*
c) *Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*Anexo 1. 49-50* *Anexo 2. 106-108* *Anexo 3. 165* *Anexo 4. 214-215* *Anexo 5. 270-272* *Anexo 6. 333-334* *Anexo 7. 398-399* *Anexo 8. 462-465* *Anexo 9. 534-536* *Anexo 10. 589-590*
d) *Políticas de Respaldos*	*Las políticas de respaldo contienen información del momento que se hacen los respaldos, así como la ubicación física de estos, que podrían ocasionar la pérdida, destrucción no autorizada, robo, copia no autorizada, uso, acceso o tratamiento no autorizado, el daño la alteración o modificación no autorizada de datos personales.*	*Anexo 1. 65-66* *Anexo 2. 127-128* *Anexo 3. 182-183* *Anexo 4. 230-232* *Anexo 5. 287-289* *Anexo 6. 352-354* *Anexo 7. 412-413* *Anexo 8. 486-488* *Anexo 9. 557-560* *Anexo 10. 604-606*
e) *Medidas de Seguridad*	*Las medidas de seguridad técnicas contienen las acciones implementadas o por implementar para proteger los datos*	*Anexo 12. 618-705*

Técnicas	*personales que se encuentren en formato digital, así como de los sistemas informáticos que les dan tratamiento.*	

Los fundamentos y motivos se exponen a continuación:

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

- *Divulgar el análisis de riesgo, el análisis de brecha, las políticas de respaldo, el plan de trabajo y medidas de seguridad técnicas de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

- *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha, las políticas de respaldo, el plan de trabajo y medidas de seguridad técnicas de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

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

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

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

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

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

XI. Mediante oficio **DGCS/016/2022**, recibido fecha 22 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General de Comunicación Social** informó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[5]; exige elaborar versión pública del documento de seguridad de esta área universitaria.

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

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

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

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

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	
b) Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	
c) Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de*	

	brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.	

Los fundamentos y motivos se exponen a continuación:

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

- *Divulgar el análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

- *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

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

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

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

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

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

XII. Mediante oficio **ICML/DIR/241/2022**, recibido con fecha 23 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, el **Instituto de Ciencias del Mar y Limnología** informó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[6]; exige elaborar versión pública del documento de seguridad de esta área universitaria.

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

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

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

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

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
Anexo 1. Inventario de sistemas de tratamiento de datos personales	*Se testaron algunas partes del inventario de los sistemas de tratamiento de datos personales, las cuales contienen información sobre las rutas de acceso a soportes digitales de la información y cuentas, los cuales pueden ser utilizados para un ataque informático a los activos críticos y no críticos.*	*11, 13, 26 y 36*
Anexo 2. Estructura y descripción de los sistemas de tratamiento de datos personales	*Se testaron algunas partes de la estructura y descripción de los sistemas de tratamiento de datos personales, las cuales contienen información sobre las rutas y métodos de acceso a soportes digitales y físicos de la información y la descripción y características de los lugares de resguardo, los cuales pueden ser utilizados para un ataque a los activos críticos y no críticos. Adicionalmente, los diagramas de arquitectura contenidos en dicho anexo contienen flujo de*	*43-49*

	información entre los componentes, sus rutas de acceso a soportes digitales y describe las medidas de seguridad implementadas, información que poder ser utilizada para un ataque informático a los activos críticos y no críticos.	
Anexo 3. Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*50-66*
Anexo 4. Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*67-96*
Anexo 5. Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*97-98*

Los fundamentos y motivos se exponen a continuación:

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

- *Divulgar el inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planemos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

- *En este sentido la revelación de la información que obra el inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

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

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

En tal sentido, proteger la información de los documentos relativos al inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área se adecua al principio de proporcionalidad porque se justifica

negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

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

XIII. Mediante oficio **CGEP/0493/2022**, recibido con fecha 23 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Coordinación General de Estudios de Posgrado** informó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[7]*; exige elaborar versión pública del documento de seguridad de esta área universitaria.*

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

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

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

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/529/2022

Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) Estructura y descripción de los sistemas de tratamiento de datos personales	*La estructura y descripción de los sistemas de tratamiento de datos personales, refiere especificidades de cada uno de los sistemas a cargo de esta área, como son: la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo. El uso de esta información podría ocasionar ataques informáticos dirigidos particularmente a los sistemas que resguarden el catálogo de datos personales que resulten de mayor interés para la comisión de un ilícito.*	*16 a 18*
b) Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*18 a 20*
c) Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*20*
d) Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*21*

e) Medidas de seguridad implementadas	*Con las medidas de seguridad se darían a conocer aspectos relacionados con los sistemas e infraestructura con los que cuenta esta área universitaria, así como el dictamen del análisis de vulnerabilidades de la información en los que se enuncian el inventario de sistemas, puertos de comunicación, versiones y características de las comunicaciones y equipos integrados a la red de datos, e incluso los mecanismos de seguridad y de control de la información.*	*21 a 25*
f) Mecanismos de monitoreo y revisión de medidas de seguridad	*Los mecanismos de monitoreo y revisión de medias de seguridad indican las herramientas que son utilizadas para el monitoreo de la protección de datos, así como la periodicidad en la que se realiza la revisión correspondiente, por lo que, existe un riesgo en que dicha información se utilizada para que a través de ingeniería inversa o procesos análogos se tenga acceso a los sistemas de tratamiento de datos personales.*	*25*

Los fundamentos y motivos se exponen a continuación:

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

- *Divulgar los apartados consistentes en la estructura y descripción de los sistemas de tratamiento de datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, las medidas de seguridad implementadas en esta dependencia y los mecanismos de monitoreo y revisión de dichas de seguridad, evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de*

seguridad administrativas, físicas y técnicas planemos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.

- *En este sentido la revelación de la información que obra en los apartados consistentes en la estructura y descripción de los sistemas de tratamiento de datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, las medidas de seguridad implementadas en esta dependencia y los mecanismos de monitoreo y revisión de dichas de seguridad, revelan y hacen identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

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

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

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

Por tales motivos, respetuosamente, se propone la reserva de cada uno de esos apartados que obran en el documento de seguridad de esta área universitaria (anexo), por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

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

XIV. Mediante oficio **DGAJ/SP/DCS/6577/2022**, recibido con fecha 23 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General de Asuntos Jurídicos** informó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[8]*; exige elaborar versión pública del documento de seguridad de esta área universitaria.*

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

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

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran en el Sistema de Gestión

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

de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*Numeral 3, páginas 77 a 89.*
b) Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*Numeral 4, páginas 90 a 93.*
c) Plan de Trabajo y Medidas de seguridad que hagan evidente vulnerabilidades	*El plan de trabajo y las medidas de seguridad que hagan evidente vulnerabilidades, definen los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.*	*Numeral 5, páginas 94 a 99 y numeral 6, fracción I, páginas 100 y 101, fracción III, numerales 1, 2, 3, 4, 5 y 6 páginas 102 y 103, fracción IV, numeral 3, cuatro líneas de la página 104, fracción V, numeral 2, página 105,*

		fracciones VII, VIII y IX, página 106.

Los fundamentos y motivos se exponen a continuación:

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

II. *Divulgar el análisis de riesgo, el análisis de brecha … así como el plan de trabajo y las medidas de seguridad de esta dependencia universitaria evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planemos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

III. *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha … así como el plan de trabajo y las medidas de seguridad de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta Dirección General para reaccionar ante posibles amenazas.*

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

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

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

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de ***cinco (5) años****, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.*

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

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

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

PRIMERA. Con fundamento en lo dispuesto por los artículos 10 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, así como 8, fracción VI del Reglamento de Responsabilidades Administrativas de las y los Funcionarios y Empleados de la Universidad Nacional Autónoma de México, este Órgano Colegiado rige su funcionamiento, entre otros, bajo los principios de imparcialidad, certeza, legalidad, objetividad y

profesionalismo. Por ello, al ser un asunto propuesto, entre otras Áreas Universitarias, por la **Dirección General de Asuntos Jurídicos**, dependiente de la Oficina de la Abogacía General, en este acto el Abogado General y Presidente del Comité de Transparencia, Alfredo Sánchez Castañeda, así como el Director General de Asuntos Jurídicos y Secretario Técnico de este Comité, Lic. Jorge Barrera Gutiérrez, formalmente se excusan de conocer del caso, para no afectar la imparcialidad del mismo.

SEGUNDA. De conformidad con lo dispuesto en los artículos 1, 10 y 15, fracción X del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, el Comité de Transparencia de la Universidad Nacional Autónoma de México es competente para analizar la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por la **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado y la Dirección General de Asuntos Jurídicos,** y determinar, en consecuencia, si la confirma, modifica o revoca.

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

En tal virtud la **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado y la Dirección General de Asuntos Jurídicos,** clasificaron como información reservada, por un periodo de **cinco años**, la relativa: al **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); a la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); a los Diagramas de Arquitectura; al Análisis de Riesgos; al Análisis de Brecha; al Plan de Trabajo; a la Política de Autenticación y Control de Acceso; a la Política de seguridad física y ambiental; a las Medidas de seguridad implementadas; a los Mecanismos de monitoreo y revisión de medidas de seguridad; a las Políticas de Respaldos, así como las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades**; lo anterior, conforme a lo expuesto, en cada caso, en los antecedentes VII, VIII, IX, X, XI, XII, XIII y XIV respectivamente, de la presente resolución, por actualizarse el supuesto establecido en los artículos 113, fracción

VII y 110, fracción VII de las Leyes General y Federal de Transparencia y Acceso a la Información Pública.

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

> *"… Como información reservada podrá clasificarse aquella cuya publicación:*
>
> *[…]*
>
> ***VII.** Obstruya la prevención o persecución de los delitos;*
>
> *[…]".*

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

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

Énfasis añadido.

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

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

Por otro lado, las Directrices para la prevención del delito de la Organización de las Naciones Unidas enumeran tres enfoques, a saber, la prevención social, la prevención basada en la comunidad y la prevención de situaciones propicias al delito; este último tiene por objeto reducir

las oportunidades y los incentivos para delinquir, maximizar el riesgo de ser aprehendido y reducir al mínimo los beneficios del delito. En este sentido, el enfoque de prevención de situaciones está orientada en formas específicas de delincuencia.

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

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

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

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

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

- Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
- Los incidentes y vulneraciones de seguridad ocurridas.

De conformidad con lo anterior, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, para establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, el responsable deberá monitorear y revisar de manera periódica dichas medidas, donde no podrán pasar inadvertidas las nuevas amenazas, las posibles vulnerabilidades, los riesgos en conjunto, los incidentes y las vulneraciones de seguridad ocurridas, entre otras.

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

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

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

Además de lo anterior, de conformidad con el artículo 19, fracción I, incisos b) y c) de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, durante el tratamiento automatizado de los datos personales, los sistemas de información deberán establecer las

medidas de seguridad en los periodos de inactividad o mantenimiento, así como generar respaldos y aplicar los mecanismos de control y protección para su resguardo.

Por ende, de difundirse la información contenida en los apartados relativos: **al Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); a la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); a los Diagramas de Arquitectura; al Análisis de Riesgos; al Análisis de Brecha; al Plan de Trabajo; a la Política de Autenticación y Control de Acceso; a la Política de seguridad física y ambiental; a las Medidas de seguridad implementadas; a los Mecanismos de monitoreo y revisión de medidas de seguridad; a las Políticas de Respaldos; a las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades;** así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o que **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias,** se haría del conocimiento público la falta o debilidad de seguridad en un activo o grupo de activos, físicos o electrónicos, que puede ser explotada por una o más amenazas, lo que conllevaría a la materialización de las mismas y ocasionar la pérdida, destrucción no autorizada o incluso la sustracción de los datos personales en posesión de la Universidad, así como el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, además del daño, alteración o modificación no autorizada, incluso impidiendo su recuperación, vulnerando así la seguridad de los datos personales.

Bajo estos argumentos se advierte que la clasificación de la información contenida en: el **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); los Diagramas de Arquitectura; el Análisis de Riesgos; el Análisis de Brecha; el Plan de Trabajo; la Política de Autenticación y Control de Acceso; la Política de seguridad física y ambiental; las Medidas de seguridad implementadas; los Mecanismos de monitoreo y revisión de medidas de seguridad; las Políticas de Respaldos; las Medidas de Seguridad Técnicas;** así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o que **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, tiene como propósito evitar o prevenir la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática, la cual se encuentra prevista en el Título Noveno, Revelación de Secretos y Acceso Ilícito a sistemas y equipos de informática, Capítulo II, Acceso Ilícito a sistemas y equipos de informática, del Código Penal Federal en el cual se dispone lo siguiente:

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

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

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

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

...".

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

Por lo que de darse a conocer la información relativa: al **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); a la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); a los Diagramas de Arquitectura; al Análisis de Riesgos; al Análisis de Brecha; al Plan de Trabajo; a la Política de Autenticación y Control de Acceso; a la Política de seguridad física y ambiental; a las Medidas de seguridad implementadas; a los Mecanismos de monitoreo y revisión de medidas de seguridad; a las Políticas de Respaldos; a las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades**, así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder de las Áreas**

Universitarias, la cual se encuentra contenida en los documentos de seguridad remitidos por las Áreas Universitarias, se darían a conocer las acciones implementadas o por implementar, de acuerdo con el análisis de riesgos y de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer, así como las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser: hardware, software, personal del responsable, manejo de documentos físicos y/o electrónicos, entre otros, lo que representa para las Áreas Universitarias un riesgo evidente para la estabilidad de la ejecución de las medidas de seguridad adoptadas para resguardar los datos en su poder, en tanto la publicación de esa información revelaría elementos que de manera concatenada con otra información que pudiera generarse o que se haya generado, evidenciaría vulnerabilidades que pudieran ser aprovechadas por personas dedicadas a la comisión de conductas ilícitas y con ello poner en riesgo la seguridad de los datos personales tratados en el desempeño y/o ejercicio de sus competencias, facultades y/o funciones.

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

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

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

> *"Artículo 104. En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:*
>
> *I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;*
> *II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y*
> *III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio".*

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

De difundirse la información contenida en el **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); los Diagramas de Arquitectura; el Análisis de Riesgos; el Análisis de Brecha; el Plan de Trabajo; la Política de Autenticación y Control de Acceso; la Política de seguridad física y ambiental; las Medidas de seguridad implementadas; los Mecanismos de monitoreo y revisión de medidas de seguridad; las Políticas de Respaldos; las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades,** así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, representa un riesgo potencial para las Áreas Universitarias, pues a través de dicha información se podrían identificar vulnerabilidades que pueden ser aprovechadas para realizar conductas contrarias a derecho, tales como actos vandálicos, o bien, ataques informáticos de diversa índole, disminuyendo la capacidad de las Áreas Universitarias para responder ante posibles amenazas.

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

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

El perjuicio que en su caso ocasionaría al interés público la divulgación de la información en cuestión, supera al perjuicio que se ocasionaría al no publicarla, pues con la difusión de la información contenida en el **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); los Diagramas de Arquitectura; el Análisis de Riesgos; el Análisis de Brecha; el Plan de Trabajo; la Política de Autenticación y Control de Acceso; la Política de seguridad física y ambiental; las Medidas de seguridad implementadas; los Mecanismos de monitoreo y revisión de medidas de seguridad; las Políticas de Respaldos; las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades,** así como **toda**

aquella información que se encuentre directamente relacionada con alguno de dichos apartados o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, se limitaría la capacidad de las Áreas Universitarias para prevenir la comisión de conductas ilícitas.

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

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

Se considera que la limitación de acceso a la información solicitada se ajusta al principio de proporcionalidad, toda vez que se justifica negar su acceso, a cambio de garantizar la capacidad de las Áreas Universitarias para implementar todas aquellas medidas y acciones tendientes a reducir el riesgo de que se cometa una conducta ilícita que pudiera vulnerar los datos personales cuyo tratamiento realizan las Áreas Universitarias, en el desempeño y/o ejercicio de sus competencias, facultades o funciones.

En ese sentido, se considera que la limitación representa el medio menos restrictivo disponible para evitar el perjuicio ya que únicamente se restringirá el acceso a la información por un periodo de **cinco años**, el cual se computará a partir de la fecha en que se emite la presente resolución y hasta la fecha de término del periodo, o bien, se interrumpirá antes si desaparecen las causas que originaron la reserva de la información, lo que suceda primero. De tal forma que no se afecte la capacidad de este sujeto obligado para prevenir la comisión de conductas ilícitas, pero tampoco se prive de manera trascendente el acceso a la información, en su momento, ya que éste no se verá restringido por un periodo mayor al previsto por la norma.

Por lo antes mencionado, se colman las hipótesis de las fracciones I, II y III, dispuestas en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, por lo que es procedente **CONFIRMAR** la reserva total de una parte de la información para la elaboración de la versión pública propuesta por la **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado y la Dirección General de Asuntos Jurídicos,** por un periodo de **cinco años**, que se computarán a partir de la fecha de la presente resolución, de conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

CUARTA. Este Comité considera pertinente orientar a las Áreas Universitarias, a efecto de que en la elaboración de la versión pública de sus respectivos documentos de seguridad, tengan en cuenta lo siguiente:

- Deberán testar las secciones o información correspondientes al **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); a la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); a los Diagramas de Arquitectura; al Análisis de Riesgos; al Análisis de Brecha; al Plan de Trabajo; a la Política de Autenticación y Control de Acceso; a la Política de seguridad física y ambiental; a las Medidas de seguridad implementadas; a los Mecanismos de monitoreo y revisión de medidas de seguridad; a las Políticas de Respaldos; a las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en su poder**; para lo cual deberán emplear un medio que no permita la visualización de la misma y que no impida la lectura de aquella información que no es considerada como reservada. Al respecto, es importante precisar que **no deberán suprimirse las secciones** donde se contenga la información objeto de reserva.

- Deberán insertar un cuadro de texto en el cual se indiquen:

  - Las partes o secciones reservadas.
  - El fundamento legal que sustenta la reserva, así como el plazo de ésta, mismos que se encuentra indicados en el último párrafo de la consideración **TERCERA** de la presente resolución.

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

Por lo expuesto, y con fundamento en lo dispuesto por los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 1, 6, 7, 8, 23, 44, fracción II, 113, fracción VII, 137 inciso a) de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 110, fracción VII, y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública; 1, 15, fracción X, 38, último párrafo del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, este Comité de Transparencia:

R E S U E L V E

PRIMERO. Con fundamento en lo dispuesto en los artículos 1, 10, 11, 15 fracción X y 31, fracción I del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, 137, inciso a) de la Ley General de Transparencia y Acceso a la Información Pública y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia **CONFIRMA** la **CLASIFICACIÓN** de **RESERVA** total de una parte de la información, para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por la **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado y la Dirección General de Asuntos Jurídicos,** en relación con: el **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); los Diagramas de Arquitectura; el Análisis de Riesgos; el Análisis de Brecha; el Plan de Trabajo; la Política de Autenticación y Control de Acceso; la Política de seguridad física y ambiental; las Medidas de seguridad implementadas; los Mecanismos de monitoreo y revisión de medidas de seguridad; las Políticas de Respaldos; las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, por un periodo de **cinco años**, contados a partir de la fecha de la presente resolución, o bien, hasta en tanto se extingan las causas que dieron origen a la reserva de la información.

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

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

TERCERO. Con fundamento en los artículos 45, fracción V y 137, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública: así como 53, fracción VI, inciso c) del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, notifíquese la presente resolución por correo institucional a la **Coordinación de Servicios Administrativos Morelos,** a la **Coordinación de Vinculación y Transferencia Tecnológica,** a la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** a la **Dirección General de Repositorios Universitarios,** a la **Dirección General de Comunicación Social**, al **Instituto de Ciencias del Mar y Limnología,** a la **Coordinación General de Estudios de Posgrado,** a la **Dirección General de Asuntos**

Jurídicos, así como a la Unidad de Transparencia de esta Universidad, para los efectos procedentes.

Así lo resolvió por unanimidad de votos de sus integrantes, el Comité de Transparencia de la Universidad Nacional Autónoma de México, en términos de los artículos 1, 11, 15, 20 y 53, fracción VI del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

POR MI RAZA HABLARÁ EL ESPÍRITU"
Ciudad Universitaria, Cd. Mx., 24 de agosto de 2022

Archivo	03-ctunam-529-2022-docto-seg-4.pdf		
Identificador único (hash)	7ea1352b88c3430d8fed8338941833551612904 0e57b16f3d4c8dadf738fabe9		
Fecha y hora de cierre	24/08/2022 19:14:12	**Fecha y hora de emisión**	24/08/2022 19:35:46
Número de páginas	42	**Firmantes**	5

Firmantes

Nombre	Lic. MARIA ELENA GARCIA MELENDEZ	**Fecha y hora de firma**	24/08/2022 16:08:25
Directora General para la Prevención y Mejora de la Gestión Institucional y Suplente del Contralor			
Hash Firma	af63b93b888bc04e10a2246f6609ccd5cf4c5136859d7432285e4b32d6301d670ca81bf6e5dd3f98e0f50ef4b5ca130f		

Nombre	Dra. Guadalupe Barrena Nájera	**Fecha y hora de firma**	24/08/2022 16:36:33
Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género			
Hash Firma	934427d85bb1890d0ba0b7038eae904df96ad6004d5058b5cca1c8a2f887ec4bd06c8d86465ff3ff367c42f4c0684937		

Nombre	Ing. Ricardo Ramírez Ortiz	**Fecha y hora de firma**	24/08/2022 15:52:42
Director General de Servicios Generales y Movilidad			
Hash Firma	c192cd7805a02e4223fb9c95b3ff52b73d61fa338708aeccf4dda623b8f47e5b4b436deca270e424ba4eaf7dde9f6089		

Nombre	JOSE MELJEM MOCTEZUMA	**Fecha y hora de firma**	24/08/2022 17:57:01
Titular de la Unidad de Transparencia			
Hash Firma	e826eb06c8e40bfbed24f0f81ab50624c871e30f1085bd4b37991331c936ed4965a7b9b4ff85ae52896a51fc145d02ef		

Nombre	Dra. Jacqueline Peschard Mariscal	**Fecha y hora de firma**	24/08/2022 19:14:12
Especialista			
Hash Firma	155d4b30a5034a8da015b961a57db05b2ec0bf0832913877034d642ce5cd3ba748a5f504ad999eab93165beb93861fd3		