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

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Ciudad Universitaria, CDMX., a 15 de enero de 2024

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 (UNAM) como Sujeto Obligado para cumplir con los principios, deberes y demás obligaciones reconocidas por dicha Ley.

Bajo este contexto, el artículo 35 de la Ley General, 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 precepto legal antes invocado, 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), Sistema de Control de Asistencia (SCA) y Sistema de Videovigilancia (SVV).

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES.

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, así como 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 los asuntos 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 la DGAJ, logrando de esta manera desahogar con mayor celeridad los asuntos, reduciendo los tiempos de turnado.

Dirección General de Asuntos Jurídicos	
Identificador único:	**SIGAR**
(Nombre del sistema A1) *	**Sistema de Gestión de Asuntos Recibidos**
Datos Personales (sensibles o no) contenidos en el sistema	**Finalidad**
• Afiliación sindical. • Afore. • Bienes muebles e inmuebles. • Cadena original del complemento de certificación digital del SAT. • 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.	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 administrativas y universitarias y a los órganos colegiados.

Datos Personales (sensibles o no) contenidos en el sistema	Finalidad
• Certificado de sello digital - Servicio de Administración Tributaria (SAT). • Certificados y reconocimientos, entre otros. • Clave de Elector del INE • Clave Única de Registro de Población (CURP). • Código postal. • Correo electrónico personal. • Costumbres. • Creencias religiosas, filosóficas y morales. • Cuenta bancaria, número de cuenta bancaria y/o clabe 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 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	

Datos Personales (sensibles o no) contenidos en el sistema	Finalidad
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 académica. • 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. • Número de cédula de identidad, cualquiera que sea su denominación. • Número de cuenta de alumno o número de matrícula escolar. • Número de licencia de conducir.	

Datos Personales (sensibles o no) contenidos en el sistema	Finalidad
• 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. • Ocupación y/o estatus laboral de persona física. • 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 de personas físicas (RFC). • Secretos comerciales, industriales, fiscales, bancarios y fiduciarios, así como derecho de la propiedad intelectual (patentes y derechos de autor, entre otros). • Seguros.	

Datos Personales (sensibles o no) contenidos en el sistema	Finalidad
• Sello del comprobante fiscal digital por internet (CFDI). • Sello digital y/o código bidimensional. • Sexo.	

Responsable 1:	
Nombre:	**RODRÍGUEZ GONZÁLEZ NORMA ELISA**
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 para 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. • 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. • Coordinar el acceso, consulta y, en su caso, transmisión de datos personales en el SIGAR con que cuenta la Oficina Central de Correspondencia. • 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

Responsable 1:	
	una probable vulneración a los datos personales. • Cumplir con las medidas de seguridad implementadas por la Dirección General. • Instruir al personal de la Oficina Central de Correspondencia encargado de resguardar los datos personales de no proporcionar información a personas no autorizadas.

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 alguna 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. • 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.

Responsable 2:	
	• 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:	

Usuarios:	
Nombre del Usuario 1	**ARMENDÁRIZ LÓPEZ JESÚS ALFREDO**
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. • 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

Usuarios:	
	los datos personales.
Nombre del Usuario 2	**GARCÍA SERRANO SALVADOR**
Cargo:	ASISTENTE DE PROCESOS
Funciones:	• Integrar el registro de correspondencia oficial que le sea entregada, con la finalidad de recabar y procesar la documentación recibida en la Oficina Central de Correspondencia. • Registrar y capturar en el SIGAR la correspondencia que llega de manera electrónica. • Registrar y capturar en el SIGAR toda la correspondencia recibida en la DGAJ, posterior a lo cual el propio sistema le asignará un 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.
Nombre del Usuario 3	**GARCÍA CASTILLO ILIANA**
Cargo:	DIRECTORA 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.

	Usuarios:
	• 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	**FERNÁNDEZ LOYA VICENTE MANUEL**
Cargo:	DIRECTOR DE ASUNTOS LABORALES CONTENCIOSOS.
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.

Usuarios:	
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	**CORONEL RIVERA YESICA MARIBEL**
Cargo:	DIRECTORA DE PROPIEDAD INTELECTUAL
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.

	Usuarios:
	• 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	**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. • 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

Usuarios:	
	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	**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. • 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.

Usuarios:	
Nombre del Usuario 8	**SALDÍVAR RÍOS HÉCTOR ISMAEL**
Cargo:	JEFE DE LA 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. • 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 9	**RIVERA MENDOZA ERICK URIEL**
Cargo:	JEFE 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.

	Usuarios:
	• 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 10	**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.

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 11	**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. • 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 12	**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. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.

Usuarios:	
Nombre del Usuario 13	**GIJÓN ROJAS CELESTINO CÉSAR**
Cargo:	JEFE 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 14	**ACOSTAVIQUES ORTÍZ JORGE**
Cargo:	JEFE DEL DEPARTAMENTO CONTENCIOSO LABORAL
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	**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 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 16	**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. • 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 17	**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. • 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 18	**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 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 19	**MARTÍNEZ MUÑOZ LIZBETH BETZAI**
Cargo:	JEFA DEL DEPARTAMENTO DE COMISIONES MIXTAS
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 20	**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.

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 21	**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

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 22	**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.

Usuarios:	
Nombre del Usuario 23	**ROSALES VELASCO DIEGO ARMANDO**
Cargo:	JEFE DEL DEPARTAMENTO DE COMITÉ DE TRANSPARENCIA
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 24	**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

	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 25	**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 26	**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. • 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 27	**JÁUREGUI VARGAS MÓNICA N.**
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. • Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.

Usuarios:	
Nombre del Usuario 28	**NÚÑEZ ALARCÓN SAÚL**
Cargo:	JEFE 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 29	**GÓMEZ HERRERA ILDEFONSO SALVADOR**
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

Usuarios:	
	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 30	**SALAZAR CURIEL BRUNO CÉSAR**
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

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 31	**LOZANO RAMÍREZ JOSÉ RAMÓN**
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 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	**OCHOA HERMENEGILDO RODOLFO**
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

	Usuarios:
	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 33	**VEGA ALVARADO ESTEFANIA**
Cargo:	SECRETARIA 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

	Usuarios:
	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 34	**PALACIOS PINEDA MARÍA GUADALUPE**
Cargo:	SECRETARIA 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	**PICHARDO MARTINEZ ALMA BLANCA**
Cargo:	SECRETARIO 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	**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.

	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 37	**ROSAS DELGADO JESÚS MANUEL**
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

Usuarios:	
	personales.
Nombre del Usuario 38	**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. • 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	**BORJA DE LA SANCHA DAISY CAROLINA**
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 40	**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

Usuarios:	
	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	**BERROCAL GONZÁLEZ NALLELI**
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 42	**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.

	Usuarios:
	• 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	**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.

	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 44	**VILLAGÓMEZ PELAEZ FRANCISCO MIGUEL**
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 45	**CORTÉS HERNÁNDEZ IRVIN YADIR**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos.

	Usuarios:
	• 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 46	**MICHEL PÉREZ ANA DAFNE**
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.

	Usuarios:
	• 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	**GARCÍA ORTEGA MARÍA DEL REFUGIO**
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.

Usuarios:	
Nombre del Usuario 48	**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 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	**SÁNCHEZ VÁZQUEZ EDUARDO**
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.

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 50	**BECERRIL CORDOVA LIZETH**
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.

	Usuarios:
	• Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 51	**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. • 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.

	Usuarios:
	• 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 53	**BARANDA ORTEGA HORACIO**
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 54	**VENEGAS GALLEGOS EDUARDO**
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 55	**HERNÁNDEZ ORTIZ MARÍA ANGÉLICA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos.

	Usuarios:
	• 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	**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.

	Usuarios:
	• 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	**NAVARRO ROCHA NAYELI**
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.

Usuarios:	
Nombre del Usuario 58	**VELÁZQUEZ JARAMILLO MAYVI DANIELA**
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	**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. • 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 60	**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 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 61	**RODRÍGUEZ LEAL 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 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	**SUAREZ ORTEGA KARINA ELIZABETH**
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.

	Usuarios:
	• 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	**VILLALOBOS CÁRDENAS HÉCTOR**
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 64	**SILVA OLIVER JORGE OSVALDO**
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 65	**CHÁVEZ ROBLES FRANCISCO**
Cargo:	ABOGADO AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos.

	Usuarios:
	• 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 66	**ZARAGOZA 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.

	Usuarios:
	• 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	**ÁLVAREZ OCHOA DANIEL ENRIQUE**
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.

Usuarios:	
Nombre del Usuario 68	**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. • 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	**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.

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 70	**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.

Usuarios:	
	• Informar a su superior jerárquico cuando ocurra o se detecte una posible vulneración a los datos personales.
Nombre del Usuario 71	**VELÁZQUEZ DAZA LAURA ANABEL**
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 72	**ZAMUDIO RAMÓN BRENDA**
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.

	Usuarios:
	• 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 73	**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 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 74	**CALDERÓN VÁZQUEZ CÉSAR ENRIQUE**
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 75	**CARRADA QUINTANA LORENA**
Cargo:	ABOGADA AUXILIAR
Funciones:	• Resguardar física y/o electrónicamente los datos personales de los asuntos que le sean transferidos.

	Usuarios:
	• 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	**MENDOZA MENDOZA CRISTIAN FERNANDO**
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.

	Usuarios:
	• 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	**JIMENEZ 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.

Usuarios:	
Nombre del Usuario 78	**GUERRERO ROMERO ANA 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. • 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 79	**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. • 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 80	**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 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 81	**EPIFANIO VIXTHA JESSICA 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 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 82	**PÉREZ LOZA MANUEL**
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.

	Usuarios:
	• 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 83	**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. • 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 84	**YAÑEZ PINEDA IVÁN**
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 85	**RAMÍREZ CRUZ YESSICA**
Cargo:	ASISTENTE DE PROCESOS
Funciones:	• Llevar el control y registro de entrada y salida de la documentación que debe integrarse al SIGAR.

	Usuarios:
	• 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 86	**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.
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 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 87	**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.

Usuarios:	
Nombre del Usuario 88	**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. • 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 89	**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.

	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 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 90	**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.

Usuarios:	
Nombre del Usuario 91	**HUERTA CORTÉS FABIOLA NURI**
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.

SISTEMA DE CONTROL DE ASISTENCIA (SCA)

El Sistema de Control de Asistencia recaba la información referente a la asistencia de los empleados de la dependencia a través de lectores biométricos. La información registrada puede ser consultada en el SCA, además de generar reportes en distintos formatos para su manejo y seguimiento.

El Sistema tiene como objetivo principal registrar fecha y hora de asistencia de los empleados de la dependencia, para utilizar dicha información como apoyo en las labores administrativas de la Dirección, información que es necesaria para el cumplimiento de obligaciones específicas de la DGAJ y de los trabajadores en el ámbito laboral.

Dirección General de Asuntos Jurídicos	
Identificador único:	**SCA**
(Nombre del sistema A2)	**Sistema de Control de Asistencia**
Dato Personal (sensibles o no) contenidos en el sistema	**Finalidad**
• Huella digital • Nombre de trabajadores	Usarse como método de identificación personal de los empleados de la dependencia para efecto de registro de asistencia.

Responsable 1:	
Nombre:	**VÁZQUEZ DÍAZ ARMANDO**
Cargo:	Jefe del Departamento de Informática
Funciones:	• Registrar en el sistema los datos personales de los usuarios. • Implementar las medidas de seguridad para la protección de los datos personales. • Informar al director general cuando ocurra una vulneración a los datos personales. • Supervisar el funcionamiento correcto del sistema. • Colaborar con el mantenimiento preventivo de los elementos físicos que integran el sistema. • Llevar a cabo el mantenimiento correctivo del sistema. • Generar reportes.
Obligaciones:	• Adoptar las medidas necesarias para garantizar la confidencialidad de la información contenida en el SCA. • Resguardar y controlar el acceso mediante usuario y

Responsable 1:	
	contraseña que le sea asignado. • Fungir como el responsable del funcionamiento técnico del SCA. • Proteger los datos personales contenidos en el SCA de accesos no autorizados. • Informar al director general cuando ocurra una vulneración a los datos personales. • Gestionar las autorizaciones para facultar a un funcionario como usuario del SCA.
Responsable 2:	
Nombre:	**SALDÍVAR RÍOS HÉCTOR ISMAEL**
Cargo:	Jefe de la Unidad Administrativa
Funciones:	• Supervisar el funcionamiento correcto del sistema. • Hacer consultas a los datos del sistema para generar reportes y llevar a cabo trámites administrativos.
Obligaciones:	• Resguardar y controlar el acceso mediante usuario y contraseña que le sea asignado. • Proteger los datos personales a los que tenga acceso. • Guardar confidencialidad respecto de los datos personales tratados.

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

Usuarios:	
Nombre del Usuario 1:	**NO aplica, no se cuenta con usuarios.**
Cargo:	
Funciones:	
Obligaciones:	

SISTEMA DE VIDEOVIGILANCIA (SVV)

El Sistema de Videovigilancia registra a través de cámaras de seguridad instaladas en circuito cerrado, la actividad que se lleva a cabo en la Dirección General de Asuntos Jurídicos, guardando videograbaciones a través de dispositivos DVR.

El sistema tiene como objetivo principal garantizar la seguridad de empleados y visitantes ante cualquier hecho que se suscite dentro de las instalaciones de la DGAJ.

Dirección General de Asuntos Jurídicos	
Identificador único:	**SVV**
(Nombre del sistema A3)	**Sistema de Videovigilancia**
Dato Personal (sensibles o no) contenidos en el sistema	**Finalidad**
• Imagen de una persona identificada o identificable	Garantizar la seguridad de la persona al encontrarse dentro de las instalaciones de la dependencia.

Responsable 1:	
Nombre:	**VÁZQUEZ DÍAZ ARMANDO**
Cargo:	Jefe del Departamento de Informática
Funciones:	• Colaborar con el mantenimiento técnico del sistema. • Implementar las medidas de seguridad para la protección de los datos personales. • Informar al director general cuando ocurra una vulneración a los datos personales. • Supervisar el funcionamiento correcto del sistema. • Llevar a cabo respaldos de la información del sistema a solicitud de las autoridades competentes.
Obligaciones:	• Adoptar las medidas necesarias para garantizar la confidencialidad de la información contenida en el SVV. • Resguardar y controlar el acceso mediante usuario y contraseña que le sea asignado. • Fungir como el responsable del funcionamiento técnico del SVV. • Proteger los datos personales contenidos en el SVV de accesos no autorizados. • Informar al director general cuando ocurra una vulneración a los datos personales.

Responsable 1:	
	• Gestionar las autorizaciones para facultar a un funcionario como usuario del SVV.
Responsable 2:	
Nombre:	**SALDÍVAR RÍOS HÉCTOR ISMAEL**
Cargo:	Jefe de la Unidad Administrativa
Funciones:	• Supervisar el funcionamiento correcto del sistema. • Llevar a cabo respaldos de la información del sistema a solicitud de las autoridades competentes.
Obligaciones:	• Resguardar y controlar el acceso mediante usuario y contraseña que le sea asignado. • Proteger los datos personales a los que tenga acceso. • Guardar confidencialidad respecto de los datos personales tratados.
Responsable 3:	
Nombre:	**ARMENDÁRIZ LÓPEZ JESÚS ALFREDO**
Cargo:	Director General de Asuntos Jurídicos
Funciones:	• Supervisar el funcionamiento correcto del sistema.
Obligaciones:	• Resguardar y controlar el acceso mediante usuario y contraseña que le sea asignado. • Proteger los datos personales a los que tenga acceso. • Guardar confidencialidad respecto de los datos personales tratados.

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

Usuarios:	
Nombre del Usuario 1:	**NO aplica, no se cuenta con usuarios.**
Cargo:	
Funciones:	
Obligaciones:	

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

Dirección General de Asuntos Jurídicos	
Identificador único:	**SIGAR**
Nombre del sistema A1:	**Sistema de Gestión de Asuntos Recibidos**
Tipo de soporte:	Físico y Electrónico
Descripción:	Soporte físico: Archivos donde están los documentos y/o expedientes. Soporte electrónico: Los datos del sistema están 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.
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.

Identificador único:	**SCA**
Nombre del sistema A2:	**Sistema de Control de Asistencia**
Tipo de soporte:	Electrónico
Descripción:	Los datos del sistema se encuentran alojados en los dispositivos biométricos y en la computadora de la jefatura del Departamento de Informática y en el equipo de cómputo de la jefatura de la Unidad Administrativa.
Características del lugar donde se resguardan los soportes:	Alojamiento de los datos en los dispositivos biométricos ubicados en las entradas de los Edificios A y B que comprenden la Dirección General de Asuntos Jurídicos, además de, en el equipo de cómputo ubicado en la oficina de la jefatura de la Unidad Administrativa y uno de los equipos ubicado en la oficina del Departamento de Informática.

Identificador único:	SVV
Nombre del sistema A3:	**Sistema de Videovigilancia**
Tipo de soporte:	Electrónico
Descripción:	Los datos del sistema se encuentran alojados en los discos duros de dos dispositivos DVR ubicados en el cuarto de telecomunicaciones de la DGAJ.
Características del lugar donde se resguardan los soportes:	Alojamiento de los datos en dos dispositivos DVR ubicados en el cuarto de comunicaciones de la DGAJ. Además de los respaldos, en el equipo de cómputo ubicado en la oficina de la jefatura de la Unidad Administrativa y uno de los equipos ubicado en la oficina del Departamento de Informática.

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 81 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.

Dirección General de Asuntos Jurídicos		
Identificador único:	**SIGAR**	
Nombre del Sistema A1:	**Sistema de Gestión de Asuntos Recibidos**	
RIESGOS TÉCNICOS		
Riesgo	**Impacto**	**Mitigación**
[redacted]		

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 81 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.

Dirección General de Asuntos Jurídicos	
Identificador único:	**SIGAR**
Nombre del Sistema A1:	**Sistema de Gestión de Asuntos Recibidos**
[redacted]	

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 81 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.

Dirección General de Asuntos Jurídicos	
Identificador único:	**SIGAR**
Nombre del Sistema A1:	**Sistema de Gestión de Asuntos Recibidos**
[redacted]	

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 81 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.

Dirección General de Asuntos Jurídicos		
Identificador único:	**SIGAR**	
Nombre del Sistema A1:	**Sistema de Gestión de Asuntos Recibidos**	
1		
RIESGOS ADMINISTRATIVOS Y FÍSICOS		
Riesgo	**Impacto**	**Mitigación**
1		

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 81 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.

Dirección General de Asuntos Jurídicos	
Identificador único:	**SIGAR**
Nombre del Sistema A1:	**Sistema de Gestión de Asuntos Recibidos**
1	

Dirección General de Asuntos Jurídicos		
Identificador único:	**SCA**	
Nombre del Sistema A2:	**Sistema de Control de Asistencia**	
RIESGOS TÉCNICOS		
Riesgo	**Impacto**	**Mitigación**
1		

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 81 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.

Dirección General de Asuntos Jurídicos	
Identificador único:	**SCA**
Nombre del Sistema A2:	**Sistema de Control de Asistencia**
[redacted]	

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 81 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.

Dirección General de Asuntos Jurídicos	
Identificador único:	**SCA**
Nombre del Sistema A2:	**Sistema de Control de Asistencia**
1	

RIESGOS ADMINISTRATIVOS Y FÍSICOS		
Riesgo	**Impacto**	**Mitigación**
1		

Dirección General de Asuntos Jurídicos		
Identificador único:	**SVV**	
Nombre del sistema A3:	**Sistema de Videovigilancia**	
RIESGOS TÉCNICOS		
Riesgo	**Impacto**	**Mitigación**
1		

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 81 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.

Dirección General de Asuntos Jurídicos	
Identificador único:	**SVV**
Nombre del sistema A3:	**Sistema de Videovigilancia**

1

RIESGOS ADMINISTRATIVOS Y FÍSICOS		
Riesgo	**Impacto**	**Mitigación**

1

1. Texto eliminado: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 81 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.

Dirección General de Asuntos Jurídicos	
Identificador único:	**SVV**
Nombre del sistema A3:	**Sistema de Videovigilancia**
[redacted]	

2. Texto eliminado: Apartado correspondiente a Análisis de Brecha (numeral 4, páginas 90 a 94). 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).

Ahora bien, en relación con los Sistemas de información señalados anteriormente, se comunica que, por las características de los mismos, comparten riesgos y ciertas semejanzas por lo que, en lo referente al desarrollo de este Apartado, y de acuerdo con el ámbito de nuestra competencia se analizaran de manera conjunta.

Este 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.

Dirección General de Asuntos Jurídicos		
Identificador único:	**SIGAR, SCA y SVV**	
Nombre del sistema A1, A2 y A3:	**Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia**	
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 94). 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.

Dirección General de Asuntos Jurídicos		
Identificador único:	**SIGAR, SCA y SVV**	
Nombre del sistema A1, A2 y A3:	**Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia**	
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 94). 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.

Dirección General de Asuntos Jurídicos		
Identificador único:	**SIGAR, SCA y SVV**	
Nombre del sistema A1, A2 y A3:	**Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia**	
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 94). 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.

Dirección General de Asuntos Jurídicos		
Identificador único:	**SIGAR, SCA y SVV**	
Nombre del sistema A1, A2 y A3:	**Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia**	
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 94). 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.

Dirección General de Asuntos Jurídicos		
Identificador único:	**SIGAR, SCA y SVV**	
Nombre del sistema A1, A2 y A3:	**Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia**	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
2		

3. Texto eliminado: Apartado correspondiente a Plan de Trabajo (numeral 5, páginas 95 a 101). 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.

Ahora bien, en relación con los sistemas de información señalados anteriormente, se informa que, por las características de los mismos, comparten riesgos y ciertas semejanzas por lo que, en lo referente al desarrollo de este Apartado, y de acuerdo con el ámbito de nuestra competencia se analizaran de manera conjunta.

Al definir las acciones, se deberán 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:

Dirección General de Asuntos Jurídicos			
Identificador único:	**SIGAR, SCA y SVV**		
Nombre del sistema A1, A2 y A3:	**Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia**		
Actividad	**Descripción**	**Duración**	**Cobertura**
3			

3. Texto eliminado: Apartado correspondiente a Plan de Trabajo (numeral 5, páginas 95 a 101). 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 A1, A2 y A3:	Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia		
Actividad	**Descripción**	**Duración**	**Cobertura**
3			

3. Texto eliminado: Apartado correspondiente a Plan de Trabajo (numeral 5, páginas 95 a 101). 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 A1, A2 y A3:	Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia		
Actividad	**Descripción**	**Duración**	**Cobertura**
3			

3. Texto eliminado: Apartado correspondiente a Plan de Trabajo (numeral 5, páginas 95 a 101). 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 A1, A2 y A3:	Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia		
Actividad	**Descripción**	**Duración**	**Cobertura**
3			

3. Texto eliminado: Apartado correspondiente a Plan de Trabajo (numeral 5, páginas 95 a 101). 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 A1, A2 y A3:	Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia		
Actividad	**Descripción**	**Duración**	**Cobertura**
3			

3. Texto eliminado: Apartado correspondiente a Plan de Trabajo (numeral 5, páginas 95 a 101). 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 A1, A2 y A3:	Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia		
Actividad	**Descripción**	**Duración**	**Cobertura**
3			

3. Texto eliminado: Apartado correspondiente a Plan de Trabajo (numeral 5, páginas 95 a 101). 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 A1, A2 y A3:	Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia		
Actividad	**Descripción**	**Duración**	**Cobertura**
3			

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS.

I. TRANSFERENCIAS DE DATOS PERSONALES.

Dirección General de Asuntos Jurídicos	
Identificador único:	**SIGAR, SCA y SVV**
(Nombre del sistema A1, A2 y A3)	**Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	**a)** El envío de soportes físicos se realiza a través de correspondencia ordinaria, conforme está establecido por la Unidad Administrativa. Se define un destinatario primario o secundario. **b)** Los documentos que contienen datos personales se envían en sobre o paquete sellado de manera que sea perceptible si alguien lo abrió antes de su entrega. **c)** La entrega del paquete se realizará previa acreditación con identificación oficial con fotografía del destinatario. **d)** El remitente indica si existe algún daño en el paquete que evidencie su contenido. **e)** El acuse de recibo se recaba una vez que es entregada la documentación. **f)** Se registra y digitaliza en el SIGAR el acuse de la recepción de la documentación correspondiente.
Transferencias mediante el traslado de soportes electrónicos:	**a)** El envío de soportes electrónicos se realiza a través de correspondencia ordinaria, conforme está establecido por la Unidad Administrativa. Se define un destinatario primario o secundario. **b)** Los soportes electrónicos que contienen datos personales se envían en sobre o paquete sellado de manera que sea perceptible si alguien lo abrió antes de su entrega. **c)** La entrega del paquete se realizará previa acreditación con identificación oficial con fotografía del destinatario. **d)** El remitente indica si existe algún daño en el paquete que evidencie su contenido. **e)** El acuse de recibo se recaba una vez que es entregada la documentación. **f)** Se registra y digitaliza en el SIGAR el acuse de la recepción de la documentación correspondiente. **g)** Las transferencias de datos personales no se formalizan

Dirección General de Asuntos Jurídicos	
Identificador único:	**SIGAR, SCA y SVV**
(Nombre del sistema A1, A2 y A3)	**Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia**
TRANSFERENCIAS DE DATOS PERSONALES	
	mediante instrumento jurídico, se realizan atendiendo a las excepciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Transferencias mediante el traslado sobre redes electrónicas:	**a)** El destinatario envía acuse de recibo al remitente una vez recibidos los datos personales. **b)** Las transferencias de datos personales no se formalizan mediante instrumento jurídico, se realizan atendiendo a las excepciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. El envío de los archivos de documentos que contienen datos personales se realiza a través de correo electrónico institucional, administrado por la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM. Se solicita al destinatario que envíe acuse de recibo al remitente. Cabe precisar que, la información es transferida a petición de alguna instancia pública que, de conformidad con sus atribuciones legales, así lo requiera, o bien por mandamiento judicial o ministerial.

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, menoscabo 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 y salida 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.
- 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.

1. Los datos que se registran en las bitácoras:

a) La persona que accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;

b) Para soportes físicos: Número de volante, fecha de registro, número de oficio, fecha del oficio, año, área a la que se turna, nombre y firma de quien recibe, fecha y hora de acuse, y observaciones.

c) Para soportes electrónicos: En la bitácora del SIGAR se registra el nombre del usuario que lleva a cabo un cambio en la base de datos, el tipo de movimiento que realiza, que puede ir desde el acceso o salida del sistema, modificaciones a los campos de un asunto y cambios en los documentos asociados a dichos asuntos, además de la fecha, hora y el nombre de host como identificador de la máquina desde la cual fue realizado el cambio.

2. Las bitácoras se encuentran en soporte electrónico y soporte físico.

Las bitácoras del SIGAR se encuentran en soporte electrónico en una tabla dentro de la misma base de datos del sistema.

3. Para soporte electrónico, la bitácora se encuentra en el mismo servidor donde es alojada el resto de la base de datos y por un tiempo indefinido. Para soporte físico, las bitácoras se almacenan en un librero bajo llave y se conservan atendiendo los plazos establecidos en la normatividad en materia de archivos.

4. La seguridad de la bitácora es la misma que la de los datos personales, ya que se encuentra alojada dentro de la propia base de datos, por lo tanto, cuenta únicamente con acceso a través de la red local y con las ventajas de seguridad que ofrece el gestor que la administra.

5. Para soporte electrónico y físico, el responsable de analizarlas es la propia DGAJ y el análisis se realiza, para soportes físicos por lo menos cada seis meses y para el soporte electrónico cada vez que hay modificaciones al SIGAR o alguna incidencia que amerite verificar el acceso a los datos del sistema por el Departamento de Informática.

6. Se utiliza como herramienta de análisis, según sea el caso, las consultas en lenguaje SQL a través del mismo gestor de la base de datos o software como Excel para un análisis más básico, según determine el responsable técnico del sistema.

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. En dicho informe, se precisan los soportes físicos y, en su caso, electrónicos comprometidos y, en su caso, los recuperados.

b) El incidente se registra en una hoja de cálculo, anotando quién lo resolvió, así como los

soportes dañados y recuperados. Su integridad se garantiza generando y almacenando un resumen creado y respaldándolo en un CD-R después de registrado el 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 a quien tenga facultades para presentar denuncias o querellas ante el Ministerio Público para que, en el ámbito de sus atribuciones, determine lo conducente.

d) En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen 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 los titulares involucrados, a más tardar cinco días naturales posteriores a aquél en que ocurrió el incidente, recabando el acuse de recibo de esta notificación. Adicionalmente, se les 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 dañados como, en su caso, recuperados, y
- **d)** Para soportes electrónicos: los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como, en su caso, recuperados, así como el nombre de los sistemas y de la infraestructura afectada, etc.

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

3. Su integridad se garantiza al restringir el acceso y uso de ésta, la cual se resguarda bajo llave, se genera y almacena un resumen creado para su respaldo en un CD-R. Para los soportes físicos se resguardan en una oficina bajo llave y acceso restringido a personal autorizado.

4. Para el caso de soportes electrónicos, quien autoriza la recuperación de datos es el responsable técnico del sistema, previa autorización del titular de la DGAJ.

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, el cual es 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.
- 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 oficial, que acredite 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 acreditar y autentificar su identidad.

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

Las medidas de seguridad que se han implementado para controlar el acceso a los espacios en los cuales se almacenan los soportes físicos y/o electrónicos del sistema, son las siguientes:

- Control de entrada y salida física para el personal de la DGAJ.
- Puertas con cerradura reforzada.
- Sistema de cámaras de Videovigilancia las 24 horas.

Para las personas que acceden a los espacios interiores:

1. Se identifican, autentifican y autoriza el acceso:
   - Por ser trabajador de la DGAJ, previamente registrado en el control de acceso biométrico, cuenta con la autorización para acceder a dichos espacios, a efecto de cumplir con sus funciones normativas.

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

La actualización de la información contenida tanto en el Sistema de Gestión de Asuntos Recibidos (SIGAR), como en el Sistema de Control de Asistencia (SCA), particularmente en las bases de datos, se realizará de oficio por parte del responsable del Sistema respectivo, siempre y cuando, los ajustes no incidan en el tratamiento de datos personales, conforme a los siguientes supuestos:

a) Cambio en el cargo de los usuarios del Sistema;
b) Cambio de usuarios con acceso al Sistema, y
c) Cambio en el tipo de soporte.

Es responsabilidad del titular de la Unidad Administrativa, notificar al responsable del Sistema de Tratamiento de Datos Personales, los movimientos del personal de la DGAJ para poder llevar a cabo la actualización que corresponda.

Una vez realizada la actualización solicitada, la misma quedará registrada en la bitácora correspondiente a cada Sistema.

Para la rectificación de los datos personales contenidos en los Sistemas propuestos, las personas que así lo soliciten, deberán seguir el procedimiento previsto para tal efecto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y; en los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México.

VII. PERFILES DE USUARIO Y CONTRASEÑAS.

En este rubro, se describe el esquema de perfiles de usuario y contraseñas que la Dirección General tiene implementado para el control del acceso mediante una red electrónica.

1. Modelo de control de acceso:

El modelo de control de acceso utilizado en los sistemas está basado en roles, en el cual el responsable técnico del Sistema, haciendo uso de una cuenta de usuario administrador, asigna roles a los usuarios de acuerdo a sus asignaciones de trabajo y dichos roles permiten el acceso a recursos específicos.

En el caso de los Sistemas de Control de Asistencia y Videovigilancia, se cuenta con un único rol con privilegios de administrador, por lo tanto, todos los usuarios tienen control

total de los recursos y funciones, razón por la cual únicamente los responsables de dichos Sistemas tienen acceso.

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

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
Estrictamente no. Sin embargo, los equipos de cómputo pueden compartir recursos y servicios como en un sistema operativo de red *peer to peer.*

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
Si

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
Si

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

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
Si

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
En el caso del SIGAR, no. Mientras que en los Sistemas SCA y el SVV sí.

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
El responsable técnico de los sistemas.

b) ¿Quién autoriza la creación de nuevos perfiles?
En el caso del SIGAR, el jefe inmediato del empleado al cual se le está creando un perfil.

Por lo que se refiere al SCA y al SVV, el Director General y/o el jefe de la Unidad Administrativa, en sus funciones de responsables de los sistemas.

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

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

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

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

c) ¿Cómo se evita el acceso remoto no autorizado?
El servidor que aloja la base de datos únicamente permite el acceso desde los equipos conectados a la red local.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS.

En el caso del SIGAR se realizan los siguientes procedimientos de respaldo y recuperación de datos:

1. Señalar si realiza respaldos
a) Completos _**X**_, diferenciales _**X**_ o incrementales___;
b) De forma automática ____ o Manual _**X**___,
c) Periodicidad con que los realiza: Se realiza un respaldo completo cada mes y respaldos diferenciales por semana.

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad.

Todos los respaldos se almacenan en un disco duro mecánico.

3. Cómo y dónde archiva esos medios, y

El disco duro está alojado físicamente en el servidor donde se encuentra la base de datos, esto es, en el cuarto de telecomunicaciones de la DGAJ.

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

El titular del Departamento de Informática es el responsable de realizar y resguardar los respaldos.

Para el SVV se realizan los siguientes procedimientos de respaldo y recuperación de datos:

1. Señalar si realiza respaldos
   a) Completos _**X**_, diferenciales _ o incrementales___;
   b) De forma automática _**X**__ o Manual ____,
   c) Periodicidad con que los realiza: Diariamente y se sobre escriben las Videograbaciones con duración máxima de un mes.

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad.

   Todos los respaldos se almacenan en un disco duro mecánico.

3. Cómo y dónde archiva esos medios, y

   El disco duro está alojado físicamente en dos DVR en el cuarto de telecomunicaciones de la DGAJ.

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

   La persona titular del Departamento de Informática es el responsable de verificar la correcta creación automática de los respaldos.

En tanto, para el SCA no se realiza ningún tipo de respaldo.

IX. PLAN DE CONTINGENCIA.

El Plan de contingencia para los Sistemas de Tratamiento de Datos Personales: SIGAR, SCA y SVV, se encuentra en proceso de elaboración.

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

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

Dirección General de Asuntos Jurídicos		
Identificador único:	**SIGAR, SCA y SVV**	
(Nombre del sistema A1, A2 y A3)	**Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia, Sistema de Videovigilancia**	
Recurso	**Descripción**	**Control**
Software Antivirus	Se cuenta con un software antivirus licenciado de la marca Kaspersky, del tipo *Endpoint Security,* el cual se monitorea continuamente la actividad en los equipos de cómputo de los usuarios de los sistemas.	Se tiene el software instalado con licencia activa y con las actualizaciones automáticas en la totalidad de los equipos de cómputo de la DGAJ. Se solicita a los usuarios indicar si se activa alguna alerta por contenido malicioso.

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

Dirección General de Asuntos Jurídicos		
Identificador único:	**SIGAR, SCA y SVV**	
(Nombre del sistema A1, A2 y A3)	**Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia, Sistema de Videovigilancia**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Análisis en tiempo real del Software Antivirus	Al momento de instalarse el software se activó el análisis en tiempo real, el cual se ejecuta en segundo plano en todos los equipos de cómputo analizando archivos y sitios web para identificar posibles amenazas a los recursos.	El Departamento de Informática revisa la correcta ejecución del antivirus en los equipos de cómputo con un monitoreo constante.

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

Dirección General de Asuntos Jurídicos		
Identificador único:	**SIGAR, SCA y SVV**	
(Nombre del sistema A1, A2 y A3)	**Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia, Sistema de Videovigilancia**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Análisis en tiempo real del Software Antivirus	Se ha detectado la presencia de software malicioso procedente de recursos de internet descargados por los usuarios de los equipos de cómputo.	El Departamento de Informática realiza la evaluación constante.

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

Dirección General de Asuntos Jurídicos		
Identificador único:	**SIGAR, SCA y SVV**	
(Nombre del sistema A1, A2 y A3)	**Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia, Sistema de Videovigilancia**	
Medida de seguridad*	**Acciones***	**Responsable***
Análisis en tiempo real del Software Antivirus	Revisar la correcta instalación, activación y actualización del software antivirus en los equipos de cómputo.	Las actualizaciones serán responsabilidad del Departamento de Informática con fecha límite del 5 de julio del 2024.

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.

En ese contexto, la 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.

Se solicitará a la Unidad de Transparencia para que, en conjunto con la DGTIC, impartan el Programa Universitario de Capacitación en Protección de Datos Personales, a todo el personal responsable de seguridad de datos personales e informática.

Dirección General de Asuntos Jurídicos			
Identificador único:		**SIGAR**	
(Nombre del sistema A1)		**Sistema de Gestión de Asuntos Recibidos**	
Actividad	**Descripción**	**Duración**	**Cobertura**
Exposición temática: Introducción al SIGAR y la importancia del tratamiento y protección a los datos personales contenidos en dicho Sistema.	Demostrar de forma teórica y práctica el manejo del SIGAR sensibilizando al público objetivo sobre la importancia del debido tratamiento y protección de los datos personales en el manejo del sistema.	Duración aproximada una hora.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan como **usuarios** del SIGAR.
Exposición temática: Introducción a los principios y deberes en materia de	Sensibilizar al público objetivo sobre la importancia de	Duración aproximada dos horas.	Tiene como público objetivo a todas las personas que desempeñan un cargo o

protección de datos personales.	cumplir con los principios y deberes en materia de protección de datos personales durante su tratamiento en el SIGAR.		comisión dentro de la DGAJ y que participan como **responsables y usuarios** del SIGAR.
Exposición temática: Mecanismos de protección a los datos personales tratados en el SIGAR.	Conocer, aplicar y evaluar los procedimientos más comunes que se utilizan actualmente para la protección de datos personales y su adaptación al SIGAR.	Duración aproximada una hora.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan como **responsables** del sistema SIGAR.
Exposición temática: Manejo de incidentes de seguridad de datos personales en el sistema SIGAR.	Conocer e identificar las posibles vulneraciones que se pueden presentar en el manejo del SIGAR, brindando herramientas que permitan la mitigación de las posibles consecuencias.	Duración aproximada dos horas.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan como **responsables** del sistema SIGAR.

Dirección General de Asuntos Jurídicos			
Identificador único:		**SCA**	
(Nombre del sistema A2)		**Sistema de Control de Asistencia**	
Actividad	**Descripción**	**Duración**	**Cobertura**
Exposición temática: Introducción a los principios y deberes	Sensibilizar al público objetivo sobre la	Duración aproximada dos horas.	Tiene como público objetivo a todas las personas que

en materia de protección de datos personales.	importancia de cumplir con los principios y deberes en materia de protección de datos personales durante su tratamiento en el SCA.		desempeñan un cargo o comisión dentro de la DGAJ y que participan como **responsables** del SCA.
Exposición temática: Tratamiento de datos biométricos y manejo de incidentes de seguridad de datos personales.	Conocer qué son los datos biométricos, describir sus características y analizar las circunstancias en las que pueden considerarse datos sensibles, identificando las obligaciones para el tratamiento de este tipo de datos. Así como, conocer el procedimiento a seguir ante un incidente de seguridad que permita la vulneración a dichos datos.	Duración aproximada dos horas.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan como **responsables** del SCA.
Exposición temática: Mecanismos de protección a los datos personales tratados en el SCA.	Conocer, aplicar y evaluar los procedimientos más comunes que se utilizan actualmente para la protección de datos personales y	Duración aproximada una hora.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan como **responsables** del sistema SCA.

	su adaptación al SCA.		

Dirección General de Asuntos Jurídicos			
Identificador único:		**SVV**	
(Nombre del sistema A3)		**Sistema de Videovigilancia**	
Actividad	**Descripción**	**Duración**	**Cobertura**
Exposición temática: Introducción a los principios y deberes en materia de protección de datos personales.	Sensibilizar al público objetivo sobre la importancia de cumplir con los principios y deberes en materia de protección de datos personales durante su tratamiento en el SVV.	Duración aproximada dos horas.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan como **responsables** del SVV.
Exposición temática: El derecho a la propia imagen y su importancia en el tratamiento de datos personales del SVV.	Conocer qué es el derecho a la propia imagen, ofreciendo herramientas para facilitar el cumplimiento de las exigencias en materia de protección de datos personales e identificando las obligaciones para el tratamiento de este tipo de datos.	Duración aproximada dos horas.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan como **responsables** del SVV.
Exposición temática: Mecanismos de protección a los datos personales tratados en el SVV.	Conocer, aplicar y evaluar los procedimientos más comunes que se utilizan actualmente para	Duración aproximada una hora.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan

	la protección de datos personales y su adaptación al SVV.		como **responsables** del sistema SVV.
Exposición temática: Manejo de incidentes de seguridad de datos personales en el sistema SVV.	Conocer e identificar las posibles vulneraciones que se pueden presentar en el manejo del SVV, así como describir los procesos y controles recomendados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.	Duración aproximada dos horas.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan como **responsables** del sistema SVV.

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

La difusión de la protección a los datos personales por parte de la DGAJ se realiza a través de los Avisos de Privacidad, tanto Integral como Simplificado, mediante los cuales se hace del conocimiento de los interesados, el tratamiento y finalidades que se da a dichos datos.

Dirección General de Asuntos Jurídicos			
Identificador único:		**SIGAR**	
(Nombre del sistema A1)		**Sistema de Gestión de Asuntos Recibidos**	
Actividad	**Descripción**	**Duración**	**Cobertura**
Difusión de los conceptos básicos, objetivos, mecanismos y herramientas en materia de protección de datos personales.	Se difundirá material que permita lograr una mayor comprensión del tema y el desarrollo de	La difusión se realizará de manera semestral durante un periodo de cinco días.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan como **usuarios** y

	mecanismos y habilidades para poder fortalecer el mejor tratamiento de datos personales en el manejo del Sistema, para ello, se apoyará en diversos medios como pizarrones, correo electrónico, publicaciones en la página intranet de la DGAJ, entre otros, donde se establecerán tanto la definición, como los objetivos, principios y herramientas en materia de protección de datos personales.		**responsables** del SIGAR.
Difusión de actualización del Sistema.	Se difundirá material que apoye la actualización a los usuarios que operan el Sistema, a fin de que conozcan las políticas y mecanismos de seguridad en el tratamiento de datos personales que se vayan implementando en el Sistema, e invitará al personal involucrado en el	La difusión se realizará de manera semestral durante un periodo de cinco días.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan como **usuarios** del SIGAR.

	tratamiento de datos personales a los cursos de capacitación que se efectúen según se programen por la Unidad de Transparencia.		

Dirección General de Asuntos Jurídicos			
Identificador único:		**SCA**	
(Nombre del sistema A2)		**Sistema de Control de Asistencia**	
Actividad*	**Descripción***	**Duración***	**Cobertura***
Difusión de los conceptos básicos, objetivos, mecanismos y herramientas en materia de protección de datos personales.	Se difundirá material para lograr una mayor comprensión del tema y el desarrollo de mecanismos y habilidades para poder fortalecer el mejor tratamiento de datos personales en el manejo del Sistema, para ello anterior, se apoyará en diversos medios como correo electrónico y publicaciones en la página web de la DGAJ, entre otros, donde se establecerán, tanto la definición, como los objetivos, principios y herramientas en	La difusión se realizará de manera semestral durante un periodo de cinco días.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan como **responsables** del SCA.

	materia de protección de datos personales.		
Difusión de los conceptos relacionados con la protección de datos biométricos.	Se difundirá material que apoye la sensibilización a los responsables que operan el Sistema sobre la importancia de este tipo de dato personal, con la finalidad de que conozcan los principios básicos relacionados con el tratamiento y protección de los datos biométricos.	La difusión se realizará de manera semestral durante un periodo de cinco días.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan como **responsables** del SCA.

Dirección General de Asuntos Jurídicos			
Identificador único:		**SVV**	
(Nombre del sistema A2)		**Sistema de Videovigilancia**	
Actividad	**Descripción**	**Duración**	**Cobertura**
Difusión de los conceptos básicos, objetivos, mecanismos y herramientas en materia de protección de datos personales.	Se difundirá material para lograr una mayor comprensión del tema y el desarrollo de mecanismos y habilidades para poder fortalecer el mejor tratamiento de datos personales en el manejo del Sistema, para ello se apoyará en diversos medios como correo	La difusión se realizará de manera semestral durante un periodo de cinco días.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan como **responsables** del SVV.

	electrónico y publicaciones en la página intranet de la DGAJ, entre otros, donde se establecerán tanto la definición como los objetivos, principios y herramientas en materia de protección de datos personales.		
Difusión de los conceptos básicos relacionados con el respeto al derecho de la propia imagen.	Se difundirá material que apoye la sensibilización a los responsables que operan el sistema sobre la importancia de garantizar el derecho a la propia imagen en el tratamiento que da el Sistema a este tipo de dato personal, con la finalidad de que conozcan los principios básicos relacionados con el tratamiento y protección de la imagen de una persona física.	La difusión se realizará de manera semestral durante un periodo de cinco días.	Tiene como público objetivo a todas las personas que desempeñan un cargo o comisión dentro de la DGAJ y que participan como **responsables** del SVV.

9. MEJORA CONTINUA.

9.1. Actualización y mantenimiento de Sistemas de información.

Dirección General de Asuntos Jurídicos			
Identificador único:		**SIGAR**	
(Nombre del sistema A1)		**Sistema de Gestión de Asuntos Recibidos**	
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización a una plataforma Web	Con el objetivo principal de preservar la seguridad e integridad de los datos personales almacenados en el SIGAR, así como de hacer el sistema más robusto, escalable y multiplataforma se pretende llevar a cabo la actualización.	Se llevará a cabo durante el presente año y el primer trimestre del próximo.	Se robustecerá la seguridad con tecnología más reciente, además de que los cambios solicitados serán resueltos de una manera expedita y eficiente.

Dirección General de Asuntos Jurídicos			
Identificador único:		**SCA**	
(Nombre del sistema A2)		**Sistema de Control de Asistencia**	
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento a los lectores biométricos.	Como parte del programa de mantenimiento semestral de la DGAJ, se lleva a cabo el mantenimiento preventivo de los lectores biométricos que forman parte del SCA.	Se realiza en dos días con una periodicidad semestral.	Se previene la falta de disponibilidad de los recursos ante fallas técnicas provocadas por falta de mantenimiento.

Dirección General de Asuntos Jurídicos			
Identificador único:		**SVV**	
(Nombre del sistema A3)		**Sistema de Videovigilancia**	
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento a los DVR y cámaras de Videovigilancia..	Como parte del programa de mantenimiento anual de la DGAJ, se lleva a cabo el mantenimiento preventivo de los dispositivos DVR y cada una de las cámaras que forman parte del SVV.	Se realiza en una semana con una periodicidad anual.	Se previene la falta disponibilidad de los recursos ante fallas técnicas provocadas por falta de mantenimiento.

9.2. Actualización y mantenimiento de equipo de cómputo.

Dirección General de Asuntos Jurídicos			
Identificador único:	**SIGAR, SCA y SVV**		
(Nombre del sistema A1, A2 y A3)	**Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia**		
Actividad	**Descripción**	**Duración**	**Cobertura**
Actualización de software.	Los equipos están configurados para recibir automáticamente las actualizaciones de software y se instalan según las horas activas del equipo, el Departamento de Informática realiza búsquedas manuales y periódicas de ellas.	Actividad permanente.	El 100% de los equipos de cómputo de la DGAJ

Actividad	Descripción	Duración	Cobertura
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.

Dirección General de Asuntos Jurídicos		
Identificador único:	**SIGAR**	
(Nombre del sistema A1)	**Sistema de Gestión de Asuntos Recibidos**	
Proceso	**Descripción**	**Responsable**
Respaldos de la base de datos	Se realizan respaldos con periodicidad variable o cada vez que la Dirección General solicita un corte del avance actualizado.	Departamento de Informática, ejecución máxima de 2 días hábiles.

Dirección General de Asuntos Jurídicos		
Identificador único:	**SCA**	
(Nombre del sistema A2)	**Sistema de Control de Asistencia**	
Proceso	**Descripción**	**Responsable**
No aplica.	No se realizan respaldos.	No aplica.

Dirección General de Asuntos Jurídicos		
Identificador único:	**SVV**	
(Nombre del sistema A3)	**Sistema de Videovigilancia**	
Proceso	**Descripción**	**Responsable**
Respaldos de las Videograbaciones.	Se realizan respaldos cada que la Dirección General o la Unidad Administrativa lo solicitan.	Departamento de Informática, ejecución máxima de 1 día hábil.

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

Dirección General de Asuntos Jurídicos		
Identificador único:	**SIGAR, SCA y SVV**	
(Nombre del sistema A1, AA2 y A3)	**Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia**	
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 titular del Departamento de Informática y la entrega del equipo en almacén es apoyada por el Departamento de Bienes y Suministros. El proceso completo tiene una duración máxima de 5 días hábiles.

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

Cuando la totalidad de los datos personales contenidos en un sistema de datos personales que obre en los archivos de la DGAJ hayan dejado de ser necesarios para el cumplimiento de la finalidad o finalidades para la que se recolectaron, de conformidad con lo establecido en el Aviso de Privacidad respectivo o de acuerdo a las disposiciones legales aplicables, o bien exista un sistema que otorgue un mejor tratamiento, deberán ser cancelados previo bloqueo.

El procedimiento de cancelación iniciará con el bloqueo del sistema de tratamiento de datos personales el cual se realizará por un periodo determinado atendiendo al sistema que se trate, tal como se detalla en el inciso B) del presente apartado. Corresponde al responsable de cada sistema identificar si los mismos han dejado de ser útiles e iniciar el bloqueo correspondiente de los sistemas de datos personales a cancelar previa notificación que se realice a la persona titular de la DGAJ y de la Unidad Administrativa.

La notificación que realice el responsable del sistema a cancelar deberá contener lo siguiente:

I. El nombre del sistema de datos personales a cancelar.
II. La justificación de que no existe la obligación legal de mantener por más tiempo el sistema de datos personales.
III. La justificación de que el sistema de datos personales ha dejado de ser útil.
IV. Las acciones encaminadas a recuperar, cuando sea posible, las copias o reproducciones de ese sistema de datos personales, entregados a los usuarios con el fin de evitar su tratamiento.
V. Señalar las medidas de seguridad a emplear, con el objetivo de impedir el tratamiento del sistema de datos personales durante el periodo de bloqueo.

El plazo para el bloqueo de los datos personales comienza a computarse a partir del día hábil siguiente de la notificación del responsable a las personas titulares de la DGAJ y de la Unidad Administrativa, ya que a partir de ese día, deberá impedirse cualquier tratamiento del sistema de datos personales a cancelar.

Los Sistemas de Datos Personales electrónicos almacenados en equipos de cómputo, deberán destruirse una vez concluido el periodo de bloqueo correspondiente en presencia del responsable, de las personas Titulares de la DGAJ y de la Unidad Administrativa, de un trabajador universitario adscrito al Departamento de Informática de la DGAJ, el responsable de seguridad de datos personales de la DGAJ y de un funcionario adscrito a la DGAJ que asista como testigo, para lo cual se deberá emitir un acta administrativa en donde se incluyan:

- El número de reproducciones que se tengan del sistema de datos personales;

- La especificación del tipo de base de datos (física o electrónica);
- La descripción del método de destrucción;
- El día y hora de la destrucción y
- La firma de los presentes.

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

a) Denominación: Sistema de Gestión de Asuntos Recibidos, Sistema de Control de Asistencia y Sistema de Videovigilancia.

b) Motivo de la cancelación: Cuando los datos personales contenidos en los sistemas hayan dejado de ser necesarios para cumplir la finalidad para la que se recolectaron, exista un sistema que otorgue un mejor tratamiento según las disposiciones legales aplicables.

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

A1
Por lo que hace al sistema SIGAR, el periodo de bloqueo será de dos años de acuerdo a los plazos institucionales de conservación en materia archivística, lo anterior debido a que los documentos que se producen únicamente son de apoyo informativo, es decir no se relacionan con el asunto de un expediente, carecen de valores documentales y únicamente responden a actividades asignadas al área productora.

A2 y A3
Referente al sistema SCA y SVV, el periodo de bloqueo será de cinco años considerando los plazos de prescripción para el ejercicio de un derecho por parte de los titulares de los datos.

Para llevar a cabo el bloqueo del Sistema, se deberán realizar las siguientes acciones:

1. Informar a los usuarios que el Sistema está bloqueado y poner el aviso del tratamiento de datos que se hará cuando el sistema se retire.

2. Deshabilitar el ingreso de los usuarios al Sistema.

3. Durante el bloqueo, solamente el jefe del Departamento de Informática podrá tener acceso al Sistema, en caso de que se requiera alguna información.

2. Al término del periodo de bloqueo se deberán desactivar los últimos accesos al sistema.

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

En relación con los Sistemas de información con identificadores únicos A1, A2 y A3, se comunica que, por las características de los mismos, comparten ciertas semejanzas por lo que, les son aplicables las medidas de seguridad y procedimiento para la supresión que a continuación se describen.

Una vez que comience el periodo de bloqueo, se pondrá fuera de línea el servidor y será resguardado físicamente por el Departamento de Informática, para tener acceso únicamente de forma local por el responsable técnico del sistema en caso de requerir información.

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

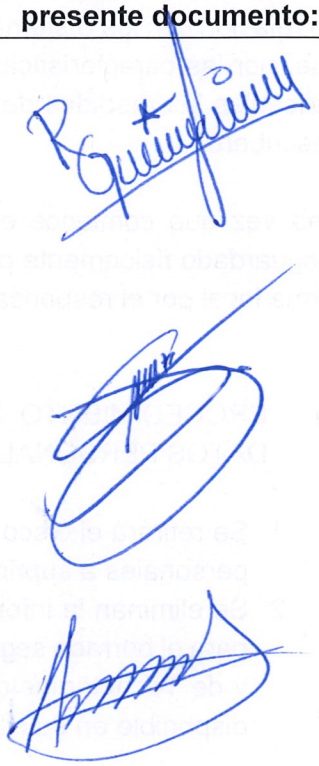
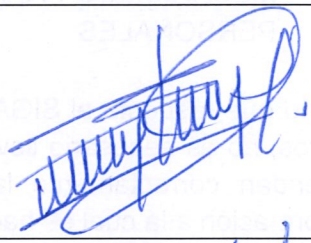
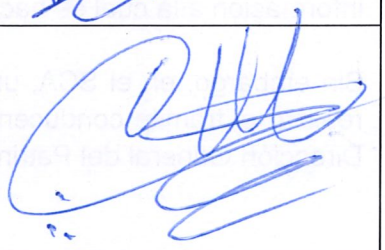
1. Se retirará el disco duro del servidor que alberga el sistema de tratamiento de los datos personales a suprimir.
2. Se eliminan la información contenida en el disco duro atendiendo las recomendaciones para el borrado seguro de la información publicadas por la Dirección General de Cómputo y de Tecnologías de la Información (DGTIC) a través de la guía con el mismo nombre disponible en su sitio web.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En lo que respecta al SIGAR y al SVV, al tratarse de sistemas alojados únicamente en discos duros, no es necesario llevar a cabo un mecanismo de supresión físico, siempre y cuando se atiendan correctamente las recomendaciones de la guía para el borrado seguro de la información a la cual se hace referencia en el punto anterior.

Sin embargo, en el SCA, una vez llevada a cabo la supresión a nivel de software, se deberá realizar el trámite conducente de baja de bienes muebles por obsolescencia o desuso ante la Dirección General del Patrimonio Universitario para los lectores biométricos.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD.

		Nombre y firma de quienes revisaron el presente documento:
Responsables del desarrollo:	Lic. Norma Elisa Rodríguez González, Coordinadora de Gestión de la DGAJ teléfono: 55562 32300, extensión: 26327, correo electrónico: dgaj@unam.mx Lic. Héctor Ismael Saldívar Ríos Jefe de la Unidad Administrativa de la DGAJ, teléfono: 5556226341, correo electrónico: dgajuadmva@unam.mx Ing. Armando Vázquez Díaz, Jefe del Departamento de Informática, 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. Jesús Alfredo Armendáriz López, Director General de Asuntos Jurídicos, teléfono: 55562 32300, extensión: 48080, correo electrónico: jarmendariz@unam.mx	
Fecha de aprobación:	15 de enero de 2024	
Fecha de actualización:	12 de agosto de 2022 15 de enero de 2024	

Partes clasificadas: Apartado correspondiente a Análisis de Riesgos (numeral 3 páginas 81 a 89), Análisis de Brecha (numeral 4, páginas 90 a 94) y Plan de Trabajo (numeral 5, páginas 95 a 101).
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: 3ª sesión ordinaria del 26/01/2024 y CTUNAM/044/2024.

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/044/2024

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 **Rectoría**, así como la **Dirección General de Asuntos Jurídicos**, en relación con su respectivo **Documento 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 permiten desarrollar el procedimiento de diseño y aplicación del sistema y procedimiento para llevar a cabo la evaluación sobre el desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resultan aplicables en la materia.

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

V. Los numerales 247 y 248 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, así como las reglas Décima Tercera y Décima Cuarta del apartado "V. Reglas de Generales de Evaluación" del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establecen que la información y documentos que se pongan a disposición de los titulares de datos personales y del Instituto, deberán ser revisados por el responsable a fin de verificar que no contengan información confidencial o reservada y, de ser el caso, deberá publicarse la versión pública de dicha documentación.

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

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

VII. A través de oficio **DGAJ/SP/DCS/516/2024**, recibido con fecha 23 de enero de 2024, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General de Asuntos Jurídicos** comunicó lo siguiente:

> *"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos 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.*
>
> *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*

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

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.

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), 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), así como 34, fracción II del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, la clasificación de la información será procedente cuando, entre otros supuestos, se determiné mediante una resolución de autoridad competente.

Por lo anterior, a efecto de cumplir con lo señalado en los preceptos antes invocados, 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 H. 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 81 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 94.*
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*	*Numeral 5, páginas 95 a 101.*

	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 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, de dar a conocer el análisis de riesgos, 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 factible 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 por un periodo de tiempo determinado, 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 ese contexto, proteger la información de los documentos relativos al análisis de riesgos, al análisis de brecha y al plan de trabajo de esta área, se adecua al principio de proporcionalidad, por lo que 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 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 ***cinco (5) años,*** *de conformidad con los artículos 32, 33, 35 y 37 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.*

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

VIII. Por oficio **3/240067**, recibido con fecha 25 de enero de 2024, dirigido a la Presidencia del Comité de Transparencia, la **Rectoría** comunicó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos 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

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

deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.

En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los 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.*	*7*
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.*	*7-8*
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.*	*8*

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 planemos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

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

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

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o

prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

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

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

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

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, junto con otra Área Universitaria, 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, Hugo Alejandro Concha Cantú, el Director General de Asuntos Jurídicos y Secretario Técnico de este Comité, Jesús Alfredo Armendáriz López, formalmente se excusan de conocer del caso, para no afectar la imparcialidad del mismo.

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

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

En tal virtud, la **Dirección General de Asuntos Jurídicos**, así como la **Rectoría** clasificaron como información reservada, por un periodo de **cinco años**, la relativa a los apartados correspondientes al **Análisis de Riesgo**, al **Análisis de Brecha** y al **Plan de Trabajo** de su respectivo Documento de Seguridad, conforme a lo expuesto en los antecedentes VII y VIII de la presente resolución, por actualizarse el supuesto establecido en los artículos 113, fracción VII y 110, fracción VII de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Por ende, de difundirse la información contenida en los apartados relativos al **Análisis de Riesgos**, al **Análisis de Brecha**, al **Plan de Trabajo**, así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o que **revele vulnerabilidades en la protección de los datos personales en poder 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, derivado de ello, ocasionar la pérdida, destrucción no autorizada o incluso la sustracción de los datos personales en posesión de la Universidad, así como el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, además del daño, alteración o modificación no autorizada, incluso impidiendo su recuperación, vulnerando así la seguridad de los datos personales.

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

> *"Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa".*
>
> *"Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*

…".

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

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

De esta forma, se colige que con la publicidad de la información referida, se generaría un riesgo potencial tanto para la documentación física como para la infraestructura tecnológica 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 señalada actualiza la causal de reserva prevista en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como en el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

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

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

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

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

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

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

La limitación se ajusta al principio de proporcionalidad, toda vez que se justifica no difundir la a información contenida en los apartados de **análisis de riesgos**, de **análisis de brecha** y del **plan de trabajo** del Documento de Seguridad, a cambio de garantizar la capacidad 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 con motivo del desempeño y/o ejercicio de sus competencias, facultades o funciones.

De igual manera, se considera que la limitación representa el medio menos restrictivo disponible para evitar el perjuicio, ya que únicamente se restringirá el acceso a la información por un periodo de **cinco años**, el cual fenecerá el **26 de enero de 2029**, o bien, se interrumpirá antes si desaparecen las causas que originaron la reserva de la información, pues durante dicho periodo podría tener lugar alguna modificación o una actualización en dichos apartados, 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, ya que éste no se verá restringido por un periodo mayor al establecido en esta resolución, el cual es acorde con lo previsto por la norma.

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

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

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

QUINTA. Las Áreas Universitarias elaborarán la versión pública de su Documento de Seguridad, teniendo en cuenta lo siguiente:

- Testar las secciones o información correspondientes al “Análisis de Riesgo”, al “Análisis de Brecha”, al “Plan de Trabajo”, así como toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en su poder; para lo cual emplearán un medio que no permita la visualización de la misma y que no impida la lectura de aquella información que no

es considerada como reservada. Al respecto, es importante precisar que **no deberán suprimirse las secciones** donde se contenga la información objeto de reserva.

- Insertar un cuadro de texto en el cual se indiquen:

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

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

Por lo expuesto, y con fundamento en lo dispuesto por los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 1, 6, 7, 8, 23, 44, fracción II, 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 y 42, primer párrafo 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 42, primer párrafo del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, 137, inciso a) de la Ley General de Transparencia y Acceso a la Información Pública y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia **CONFIRMA** la **CLASIFICACIÓN** de **RESERVA** total de la información para la elaboración de la versión pública propuesta por la **Dirección General de Asuntos Jurídicos**, así como por la **Rectoría**, en relación con los apartados de **Análisis de Riesgos**, de **Análisis de Brecha** y del **Plan de Trabajo**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, contenida en su respectivo Documento de Seguridad, por un periodo de **cinco años**, contados a partir de la fecha de la presente resolución.

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

SEGUNDO. Se instruye a las Áreas Universitarias, a fin de que verifiquen que su Documento de Seguridad contenga la información requerida y reúna las características establecidas en la normativa universitaria aplicable y, de ser el caso, sometan nuevamente a este Cuerpo Colegiado la clasificación correspondiente.

Lo anterior, de acuerdo con lo señalado en la consideración **CUARTA** de esta resolución.

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

CUARTO. Con fundamento en los artículos 45, fracción V y 137, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública; así como 42 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, notifíquese la presente resolución por correo institucional a la **Dirección General de Asuntos Jurídicos**, a la **Rectoría**, 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, 19 y 42 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

“POR MI RAZA HABLARÁ EL ESPÍRITU”
Ciudad Universitaria, Cd. Mx., a 26 de enero de 2024

Archivo	11-ctunam-044-2024-docto-seg-4.pdf		
Identificador único (hash)	8ba209b15cd55eeb0aa194484422a7e4fbc09d9e108ff69182b4c9b4fe7720ba		
Fecha y hora de cierre	26/01/2024 18:26:00	**Fecha y hora de emisión**	26/01/2024 18:32:46
Número de páginas	17	**Firmantes**	5

Firmantes

Nombre	Dra. Susana Conrada Alva Chimal	**Fecha y hora de firma**	26/01/2024 16:02:53
Dirección General de Responsabilidades, Inconformidades, Quejas y Registro Patrimonial y Suplente del Contralor			
Hash Firma	e8e2168c7599e457d36211a122f90aaeb30ba7d572df57e92597f5ca0d7b39b2ef2482e5155740c45256b2b3b217e079		

Nombre	Dra. Guadalupe Barrena Nájera	**Fecha y hora de firma**	26/01/2024 16:36:07
Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género			
Hash Firma	0d51815bbc2387760843cd01d998d15d81268897cb992b3a262840b32c70169d9fa432f58a65bbb0b95dca656db75ed6		

Nombre	Lic. Porfirio Antonio Diaz Rodríguez	**Fecha y hora de firma**	26/01/2024 17:13:50
Titular de la Dirección General de Servicios Generales y Movilidad			
Hash Firma	749dab0c15d747931c437d46fdd67b86a6ad0703e88046cb2be384339050848e590d5f041bd8fda38814422dad25232e		

Nombre	Dr. José Meljem Moctezuma	**Fecha y hora de firma**	26/01/2024 16:55:39
Titular de la Unidad de Transparencia			
Hash Firma	4791a305973acd69b20c99cfb964170442e4257b79cfe4d71741312c6ccfad043272f3905e92fe028674293dfc91e331		

Nombre	Dra. Jacqueline Peschard Mariscal	**Fecha y hora de firma**	26/01/2024 18:26:00
Especialista			
Hash Firma	969e5488da5a52d1a39db3dc04761f773474c9be5507c40c32f868af90cf29bf10fbb90bfaa759eaffa887941e1988c8		