Contenido

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

I. INTRODUCCIÓN

El derecho a la privacidad debe ser garantizado a toda persona, sin embargo, en la actualidad esta prerrogativa se encuentra en una etapa de fortalecimiento que en mucho depende de crear una cultura de protección de datos personales, esto en un contexto en que el desarrollo de las nuevas tecnologías permite la transmisión de millones de datos, en segundos, de y hacia cualquier parte del mundo sin que existan prácticamente restricciones. Es por ello que resulta necesario recordar y comprender que cada uno decide la información o actuación que desea mantener fuera de la esfera pública y, por ende, resguardada de cualquier intrusión, para ello la autodeterminación permite conservar en una zona de reserva o en un espacio de intimidad los datos personales.

En este escenario, inserto en la globalización tecnológica, existen dos niveles de responsabilidad para la protección de los datos personales; la primera a cargo de sus titulares y, la segunda, a cargo de quienes recaban y tratan ese tipo de información, sean del sector público o privado. En el primer nivel se reconoce la *autodeterminación informativa* como derecho de los titulares de los datos personales, lo cual puede interpretarse, de acuerdo a la definición del Instituto Federal de Acceso a la Información Pública (IFAI)[1], como: "… el poder de disposición y control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, así como el saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso". Por otro lado, en el segundo nivel, se encuentran quienes recaban datos personales y por ello tienen la responsabilidad de protegerlos y tratarlos exclusivamente para lo que fueron obtenidos.

[1] Protección de Datos Personales en México (2010). Consultado el 1 de junio de 2016. Visible en: http://www.controlescolar.sep.gob.mx/work/models/controlescolar/Resource/carpeta_pdf/03protecdatospersonales.pdf

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

En ese segundo nivel se encuentra la Secretaría de Desarrollo Social (SEDESOL, en lo sucesivo) que como ente público de la administración pública federal tiene como uno de sus objetivos generales el de: "Desarrollar y ejecutar programas y acciones de atención a la pobreza, vulnerabilidad y exclusión social que permitan a los sectores más desprotegidos el cumplimiento efectivo de sus derechos sociales promoviendo políticas diferenciadas de atención de acuerdo a sus necesidades"[2]. Esta tarea se cumple a través de programas sociales, en los que es necesario recabar datos personales que permitan verificar quienes cumplen con los requisitos establecidos en las reglas de operación y posteriormente elaborar padrones de beneficiarios que permitan rendir cuentas de quienes reciben apoyos por parte de esta dependencia.

Por otro lado, hay que señalar que el 26 de enero de 2017 se publicó en el Diario Oficial de la Federación la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General de Protección de Datos Personales, en adelante), normatividad que establece un marco de referencia para la protección de los datos personales en el sector público federal, estatal y municipal, así como en los tres órdenes de gobierno, incluyendo organismos autónomos, partidos políticos, fideicomisos y fondos públicos de la federación.

Derivado de lo anterior y visto que la SEDESOL obtiene datos personales para cumplir con las atribuciones que tiene asignadas en la Ley General de Desarrollo Social, es necesario atender lo establecido en el Artículo 35 de la Ley General de Protección de Datos Personales, elaborando un *Documento de Seguridad* que permita promover una Cultura de Protección de Datos Personales difundiendo los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad,

[2] Visible en el sitio web de la Secretaría de Desarrollo Social en: http://www.gob.mx/SEDESOL/que-hacemos

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

información y responsabilidad[3]; entre los responsables, encargados y usuarios de los sistemas de datos personales que existen en esta dependencia.

Es por ello que, en ejercicio de las atribuciones establecidas en los Artículos 83 y 84 de la Ley General de Protección de Datos Personales, el Comité de Transparencia de la SEDESOL emite el presente instrumento con el propósito de impulsar acciones que garanticen el derecho a la protección de datos personales promoviendo su adecuado tratamiento y como medio de difusión para que los responsables de los sistemas de datos personales conozcan y tomen las medidas que impidan su transmisión ilícita y lesiva para la dignidad y derechos de los titulares de los Datos Personales, estimando que con ello se establece un marco interno de referencia que permite la estandarización de la seguridad de los sistemas de datos personales existentes en esta dependencia.

[3] Establecidos en el Artículo 16 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

II. GLOSARIO

Áreas: Instancias de la SEDESOL previstas en su normatividad interna que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales;

Aviso de privacidad: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos;

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

Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

Comité de Transparencia (CT): Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública;

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

DGAGP: Dirección General de Atención a Grupos Prioritarios;

DGGPB: Dirección General de Geostadística y Padrones de Beneficiarios de la SEDESOL;

DGOP: Dirección General de Opciones Productivas;

DGPEO: Dirección General de Procesos y Estructuras Organizacionales;

DGPP: Dirección General de Programación y Presupuesto;

DGPS: Dirección General de Políticas Sociales;

DGRH: Dirección General de Recursos Humanos;

DGSVJF: Dirección General de Seguro de Vida para Jefas de Familia;

DGTIC: Dirección General de Tecnologías de la Información y Comunicaciones de la SEDESOL;

DGVI: Dirección General de Vinculación Interinstitucional;

Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable;

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados;

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

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

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

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

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

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

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

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

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

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

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

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

Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano;

Responsable: La SEDESOL como sujeto obligado a que se refiere el artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados a través del servidor público titular de la unidad administrativa o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales;

SEDESOL: Secretaría de Desarrollo Social;

Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;

Titular: La persona física a quien corresponden los datos personales;

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;

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

Unidad de Transparencia (UT): Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

Usuario: Servidor público facultado por un instrumento jurídico o expresamente autorizado por el Responsable que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin posibilidad de agregar o modificar su contenido, a menos que cuente con atribuciones o autorización por escrito para ello.

UMR: Unidad de Microrregiones.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

III. OBJETIVO

Contar con un documento que permita homologar las medidas de seguridad técnicas, físicas y administrativas de los diferentes sistemas de datos personales con los que cuenta la SEDESOL, para garantizar su protección, integridad y disponibilidad.

IV. MARCO JURÍDICO

Constitución Política de los Estados Unidos Mexicanos.

Ley General de Protección de Datos Personales en posesión de Sujetos Obligados.

Ley General de Transparencia y Acceso a la Información Pública.

Ley Federal de Transparencia y Acceso a la Información Pública.

V. ÁMBITO DE APLICACIÓN

Este documento es el resultado del esfuerzo conjunto entre la Dirección de Análisis e Información Institucional en funciones de la Unidad de Transparencia, la Dirección General de Tecnologías de la Información y Comunicaciones, así como la Dirección General de Geostadística y Padrones de Beneficiarios y en el se definen las medidas de seguridad administrativa, técnica y física para la protección de los sistemas de datos personales.

Por lo que una vez revisado lo dispuesto en la Ley General de Protección de Datos Personales y demás normatividad aplicable, en este documento se establecen los criterios que deberán observarse en la SEDESOL para la organización, cuidado y tratamiento de los datos personales; con el objetivo de mejorar su protección, integridad y disponibilidad; por parte de todos sus servidores públicos y, en particular, de los responsables, encargados y usuarios de cada sistema.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

VI. INVENTARIO DE DATOS PERSONALES Y LOS SISTEMAS DE TRATAMIENTO

Para estar en condiciones de determinar el inventario de datos y sistemas con los que cuenta esta dependencia se realizó una encuesta de diagnóstico en la que se consultó a las áreas que tenían registrado un sistema de datos personales en 2016 en el Sistema Persona, por lo que a partir de los resultados de este ejercicio y la clasificación que establece la Ley General de Protección de Datos Personales se tiene lo siguiente:

1.- Inventario de datos personales.

En primer lugar, es necesario establecer la clasificación de datos personales de acuerdo a la ley de la materia, misma que en su apartado de definiciones señala dos tipos.

a) **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;
b) **Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;[4]

De la clasificación citada y el resultado de la encuesta practicada se desprende que esta dependencia cuenta con el siguiente tipo de datos personales:

- Servicios contratados
- Afores
- Seguros
- Ingresos y Egresos
- Bienes muebles e inmuebles
- Referencias Personales
- Datos de origen étnico
- Nacionalidad
- Fecha y lugar de nacimiento
- Fotografía
- Edad
- CURP y RFC
- Estado civil
- Correo particular
- Domicilio y teléfono (celular o fijo) particular
- Nombres de familiares, dependientes y beneficiarios.
- Discapacidades
- Enfermedades

[4] Fracciones IX y X del Artículo 3 de la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados.

- Datos biométricos recabados por la Secretaría de Comunicaciones y Transportes en el marco del Programa de Trabajo para la Transición a la Televisión Digital Terrestre (TDT)[5]

2.- Inventario de sistemas de datos personales.

Los datos que han quedado enlistados se encuentran contenidos en los siguientes sistemas de datos personales.

No.	Nombre del SDP	UA
1	Sistema de Gestión de Afiliación de Jefas de Familia	DGSVJF
2	Argos AP	DGAGP
3	CAPFA (Captura de Fichas de Atención)	DGAGP
4	SIIPJA (Sistema Integral de Información para el Programa Agrícolas)	DGAGP
5	MOSERED	DGAGP
6	Padrón Único de Beneficiarios	DGGPB
7	Sistema de Focalización de Desarrollo (SIFODE)	DGGPB
8	ENLACENET	DGVI
9	Información Opciones Productivas	DGOP
10	SIOP- Módulos CUIS	DGOP
11	Sistema de Gestión de las Estancias Infantiles	DGPS
12	Sistema Integral de Información del Programa de Empleo Temporal	UMR
13	Expedientes de Personal	DGRH
14	Sistema de Administración de Personal	DGRH
15	Registro único de Servidores Públicos (RUSP)	DGRH
16	Sistema Integral de Administración de Personal	DGRH
17	Sistema de Honorarios	DGRH
18	Sistema de Honorarios (SIHO)	DGPEO
19	Sistema de Pagos	DGPP

[5] Esta base de datos se encuentra bloqueada y sin acceso a la misma hasta en tanto el INAI determine que se han cumplido con las recomendaciones realizadas respecto de este programa.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

VII. FUNCIONES Y OBLIGACIONES DE PERSONAS QUE TRATAN DATOS PERSONALES

1. De los responsables de sistemas de datos personales.

Los responsables, en todo momento, velaran por garantizar la confidencialidad, integridad y disponibilidad de los sistemas de datos personales que posee, para ello a continuación se enlistan de manera enunciativa, más no limitativa las siguientes funciones y obligaciones.

a) Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.
b) Tratar los datos personales para finalidades concretas, lícitas, explícitas y legítimas en ejercicio a las facultades o atribuciones que la normatividad aplicable le confiera.
c) Evitar la obtención y tratamiento de datos personales, a través de medios engañosos o fraudulentos.
d) Privilegiar la protección de los intereses del titular de los datos y la expectativa razonable de privacidad.
e) Tratar los datos personales previo consentimiento, expreso o tácito, otorgado por el titular de manera libre, específica e informada; salvo cuando se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General de Protección de Datos Personales.
f) Obtener el consentimiento expreso y por escrito del titular para su tratamiento, tratándose de datos personales sensibles, salvo en los casos previstos en el artículo 22 de la Ley General de Protección de Datos Personales.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

g) Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

h) Establecer los plazos de conservación de los datos personales tomando en consideración las finalidades que justificaron su tratamiento y las disposiciones aplicables en materia de protección de datos personales, así como los aspectos administrativos, contables, fiscales, jurídicos e históricos de los mismos.

i) Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento, previo bloqueo, en su caso, y una vez que concluya el plazo de conservación de los mismos.

j) Implantar mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, incluyendo la revisión periódica sobre la necesidad de conservar los datos personales.

k) Tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

l) Informar al titular, a través del aviso de privacidad, que deberá ser difundido por medios electrónicos y físicos, la existencia, características principales y finalidades del tratamiento al que serán sometidos sus datos personales.

m) Instrumentar medidas compensatorias de comunicación masiva cuando resulte imposible dar a conocer al titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados.

n) Establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan salvaguardarlos contra daño, pérdida,

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

o) Formalizar la relación con el Encargado mediante un contrato en el que se establezcan las obligaciones de ambos en torno a la protección de datos personales.

p) Atender, dentro de los plazos establecidos, las solicitudes de ejercicio de los derechos ARCO que les sean turnadas por la Unidad de Transparencia.

2.- De los Encargados y Usuarios de los sistemas de datos personales.

Los Encargados y Usuarios serán corresponsables de garantizar la confidencialidad, integridad y disponibilidad de los sistemas de datos personales a los que tienen acceso, para ello a continuación se enlistan de manera enunciativa, más no limitativa las siguientes funciones y obligaciones.

a) Tratar los datos personales para finalidades concretas, lícitas, explícitas y legítimas en ejercicio a las facultades o atribuciones que la normatividad aplicable le confiera o en cumplimiento a las instrucciones otorgadas por el Responsable del sistema de datos personales.
b) Privilegiar la protección de los intereses del titular de los datos y la expectativa razonable de privacidad.
c) Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.
d) Tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento o

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

en acatamiento a las instrucciones otorgadas por el Responsable del sistema de datos personales.

e) Cumplir las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan salvaguardarlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

f) Observar las indicaciones e instrucciones que el responsable del sistema de datos personales para la protección de los mismos y notificarle de inmediato en caso de que exista alguna vulneración al sistema o sistemas al que tenga acceso.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

VIII. ANÁLISIS DE RIESGOS

De acuerdo a lo que establece la fracción IV del Artículo 33 de la Ley General de Protección de Datos Personales un análisis de riesgo de los datos personales se elabora “considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros”.

En general, se considera que en toda organización, incluyendo esta Dependencia, existen los riesgos que se enlistan a continuación:

a) No contar con un documento que regule y sirva como guía para la protección de datos personales con las medidas de seguridad que deben observar quienes tratan con ellos.

b) La posibilidad de violación de derechos de los Titulares por la pérdida de sus datos personales o el daño causado por una utilización ilícita o fraudulenta de los mismos, por desconocimiento de las obligaciones legales o las medidas de protección.

En ese contexto, como un elemento necesario para identificar correctamente los riesgos, se consultó con las áreas que tienen a su cargo sistemas de datos personales para conocer su estatus actual, valorar la posibilidad de que suceda algún evento que comprometa la seguridad de la información que contienen y el daño que causarían en caso de materializarse y el resultado se presenta a continuación.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

1. En cuanto a las **medidas de seguridad físicas**, las áreas consultadas, respecto a las preguntas de cuáles son y en qué consisten, a *grosso modo*, respondieron:

a) La encargada de la seguridad física es la Dirección General de Tecnologías de la Información y Comunicación.

b) Se encuentra en un *data center*, con medidas perimetrales que cuentan con sistema biométrico de acceso, sistema de video vigilancia 24/7, control de acceso con tarjeta magnética.

c) El equipo cuenta con UPS que garantiza 2 horas más de servicio en el caso de que si el suministro eléctrico falle. El equipo se encuentra sobre una mesa aislado del resto de los equipos situación que evita un sobre calentamiento. El equipo se encuentra alojado en el *site* del 51 sitio para poder acceder se debe tener permiso a DGTIC (sic). El acceso tiene una cámara de video vigilancia, aunque se desconoce si esta activa o no.

2. En cuanto a las **medidas de seguridad técnicas**, las áreas consultadas, respecto a las preguntas de cuáles son y en qué consisten, a *grosso modo*, respondieron:

a) DGTIC es la encargada de la seguridad técnica.

b) El sistema no cuenta con actualizaciones adecuadas.

c) Las que determinen DGTIC y DGGPB.

d) La información se encuentra encriptada.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

3. En cuanto a las **medidas de seguridad administrativas**, las áreas consultadas, respecto a las preguntas de cuáles son y en qué consisten, a *grosso modo*, respondieron:

a) El acceso a la base se encuentra restringida y controlado por claves con diferentes niveles de acceso, intransferible.

b) El único acceso es mediante la red interna de Sedesol. El o los usuarios para acceder a la base se encuentra acotada. Cada movimiento dentro de la base se registra conforme al usuario que la realiza.

c) Todas las proporcionadas por la DGTIC

Para que este diagnóstico cuente con mayores elementos de valoración debe señalarse que después de hacer un recorrido por las instalaciones de los inmuebles en los que se encuentran las oficinas de la SEDESOL, se aprecia que existen una serie de medidas de seguridad, entre las más evidentes se encuentran las de carácter físico que se detallan a continuación:

- Cuerpo de vigilancia al acceso de cada edificio en el que se requiere identificación y conocer la persona que se visita, a quien se le solicita autorización para el ingreso.

- Libro de registro de visitas.

- Vigilantes en pisos que registran el nombre de la persona que ingresa (incluso siendo servidor público de la propia SEDESOL) y solicitan autorización del servidor público que es visitado.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

- Equipo de videovigilancia.
- Los equipos de cómputo tienen asignado un usuario y cada uno la contraseña con la que pueden acceder al mismo.
- De acuerdo a los niveles de responsabilidad se asignan permisos de navegación y acceso a sitios de internet.
- Los equipos con inactividad se bloquean y para reiniciar se requiere introducir la contraseña cada que esto ocurre.

De la información obtenida y la observación realizada se puede deducir que si bien existen medidas físicas, técnicas y administrativas para la protección de los datos personales, también se deduce que varios de los responsables de los sistemas desconocen las obligaciones que establece la Ley General de Protección de Datos, sus atribuciones y funciones; por ello señalan que corresponde a otros y no a ellos ser garantes de las medidas de seguridad; también se aprecia que hay una percepción limitada respecto al ámbito de aplicación de las medidas de seguridad, ya que se considera que éstas son responsabilidad del Encargado, DGTIC o la DGGPB, y, por ende, solamente las medidas administrativas les resultan aplicables.

Esta situación genera riesgos porque evidentemente el desconocimiento de las normas y las medidas de seguridad acrecienta la probabilidad de que ocurra un incidente, lo que inevitablemente puede causar un impacto con un determinado daño en los sistemas de datos personales y entre ellos deben considerarse los siguientes.

Código de identificación del riesgo (CIR)	Descripción del riesgo	Nivel de impacto si el riesgo se materializa	Probabilidad de que se materialice
CIR 1	Tratar datos personales con motivos distintos de la finalidad para los que fueron recabados o sin contar con las atribuciones o funciones para ello.	Alto	Media

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

CIR 2	Obtener un consentimiento que no cumpla con los requisitos que establece la Ley General de Protección de Datos Personales, para el tratamiento de datos personales.	Medio	Media
CIR 3	Acceso a los datos personales por parte de personas no autorizadas o sin atribuciones para ello.	Medio	Baja
CIR 4	Carencia o falta de supervisión de las medidas de seguridad de los sistemas de datos personales.	Medio	Media
CIR 5	Modificación, alteración o sustracción de datos personales por parte de personas no autorizadas o sin atribuciones para ello.	Alto	Alta
CIR 6	Desconocimiento de la necesidad de realizar procesos de Disociación para responder solicitudes de acceso a la información pública.	Medio	Baja
CIR 7	Elaboración de un contrato incompleto con el Encargado, en el que no se estipulen todos los apartados necesarios y las garantías adecuadas para la protección de los datos personales o la cláusula de confidencialidad.	Bajo	Baja
CIR 8	Dificultar el ejercicio de los derechos ARCO.	Bajo	Baja
CIR 9	Deficiente definición de funciones y competencias del Responsable, Encargado y Usuario(s).	Bajo	Alta
CIR 10	Falta de información a los servidores públicos que tienen acceso a los sistemas de datos personales sobre las medidas de seguridad que están obligados a observar y las consecuencias ante su omisión.	Medio	Alta
CIR 11	Falta de acciones para desincentivar la posibilidad de transmitir datos personales de manera ilícita por su valor (económico, político, social, laboral, etc.) para terceros no autorizados.	Alto	Baja
CIR 12	Percepción errónea de capacidad legal para el tratamiento o cesión de datos personales, incluso entre responsables sin las formalidades que requiere la Ley.	Medio	Baja

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

IX. ANÁLISIS DE BRECHA

De acuerdo a lo que establece la fracción V del Artículo 33 de la Ley General de Protección de Datos Personales un análisis de brecha consiste en comparar “las medidas de seguridad existentes contra las faltantes en la organización responsable”. En este sentido, al haberse conocido los riesgos en la seguridad de los sistemas de datos personales, es importante identificar las acciones necesarias para implantar las medidas que permitan evitar, eliminar o mitigar la probabilidad de que se materialicen y por ende impedir o reducir el impacto que podría generarse.

(CIR)	Descripción del riesgo	Medidas	Acciones
CIR 1	Tratar datos personales con motivos distintos de la finalidad para los que fueron recabados o sin contar con las atribuciones o funciones para ello.	Concientizar a las áreas responsables de SDP´s de la obligatoriedad de cumplir con el Principio de Finalidad.	-Elaborar el Documento de Seguridad, difundirlo en la SEDESOL. - Brindar capacitación y asesoría de acompañamiento de manera permanente. - Supervisar el cumplimiento de las medidas de seguridad.
CIR 2	Obtener un consentimiento que no cumpla con los requisitos que establece la Ley General de Protección de Datos Personales, para el tratamiento de datos personales.	Concientizar a las áreas responsables de SDP´s de la obligatoriedad de cumplir con el Principio de Lealtad.	-Elaborar el Documento de Seguridad, difundirlo en la SEDESOL. - Brindar capacitación y asesoría de acompañamiento de manera permanente. - Supervisar el cumplimiento de las medidas de seguridad.
CIR 3	Acceso a los datos personales por parte de personas no autorizadas o sin atribuciones para ello.	Concientizar a las áreas responsables de SDP´s de la obligatoriedad de cumplir con el Principio de Responsabilidad.	-Elaborar el Documento de Seguridad, difundirlo en la SEDESOL. - Brindar capacitación y asesoría de acompañamiento de manera permanente.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

			- Supervisar el cumplimiento de las medidas de seguridad.
CIR 4	Carencia o falta de supervisión de las medidas de seguridad de los sistemas de datos personales.	Concientizar a las áreas responsables de SDP´s de la obligatoriedad de cumplir con el Principio de Responsabilidad.	-Elaborar el Documento de Seguridad, difundirlo en la SEDESOL. - Brindar capacitación y asesoría de acompañamiento de manera permanente. .
CIR 5	Modificación, alteración o sustracción de datos personales por parte de personas no autorizadas o sin atribuciones para ello.	Concientizar a las áreas responsables de SDP´s de la obligatoriedad de cumplir con el Principio de Responsabilidad.	-Elaborar el Documento de Seguridad, difundirlo en la SEDESOL. - Brindar capacitación y asesoría de acompañamiento de manera permanente. - Supervisar el cumplimiento de las medidas de seguridad.
CIR 6	Desconocimiento de la necesidad de realizar procesos de Disociación para responder solicitudes de acceso a la información pública.	Concientizar a las áreas responsables de que la Ley General de Protección de Datos Personales son de orden público y por ende se debe garantizar la observancia de los principios de protección de DP.	-Elaborar el Documento de Seguridad, difundirlo en la SEDESOL. - Brindar capacitación y asesoría de acompañamiento de manera permanente. - Supervisar el cumplimiento de las medidas de seguridad.
CIR 7	Elaboración de un contrato incompleto con el Encargado, en el que no se estipulen todos los apartados necesarios y las garantías adecuadas para la protección de los datos personales o la cláusula de confidencialidad.	Concientizar a las áreas responsables de que la Ley General de Protección de Datos Personales son de orden público y por ende se debe garantizar la observancia de los principios de protección de DP.	-Elaborar el Documento de Seguridad, difundirlo en la SEDESOL. - Brindar capacitación y asesoría de acompañamiento de manera permanente. .
CIR 8	Dificultar el ejercicio de los derechos ARCO.	Concientizar a las áreas responsables de que la Ley General de Protección de Datos Personales son de orden público y por ende se debe garantizar la	-Elaborar el Documento de Seguridad, difundirlo en la SEDESOL. - Brindar capacitación y asesoría de

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

		observancia de los principios de protección de DP.	acompañamiento de manera permanente. - Supervisar el cumplimiento de las medidas de seguridad.
CIR 9	Deficiente definición de funciones y competencias del Responsable, Encargado y Usuario(s).	Concientizar a las áreas responsables de SDP´s de la obligatoriedad de cumplir con el Principio de Licitud.	-Elaborar el Documento de Seguridad, difundirlo en la SEDESOL. - Brindar capacitación y asesoría de acompañamiento de manera permanente. - Supervisar el cumplimiento de las medidas de seguridad.
CIR 10	Falta de información a los servidores públicos que tienen acceso a los sistemas de datos personales sobre las medidas de seguridad que están obligados a observar y las consecuencias ante su omisión.	Concientizar a las áreas responsables de SDP´s de la obligatoriedad de cumplir con el Principio de Responsabilidad.	-Elaborar el Documento de Seguridad, difundirlo en la SEDESOL. - Brindar capacitación y asesoría de acompañamiento de manera permanente. - Supervisar el cumplimiento de las medidas de seguridad.
CIR 11	Falta de acciones para desincentivar la posibilidad de transmitir datos personales de manera ilícita por su valor (económico, político, social, laboral, etc.) para terceros no autorizados.	Concientizar a las áreas responsables de SDP´s de la obligatoriedad de cumplir con el Principio de Responsabilidad, Licitud y Calidad.	-Elaborar el Documento de Seguridad, difundirlo en la SEDESOL. - Brindar capacitación y asesoría de acompañamiento de manera permanente. - Supervisar el cumplimiento de las medidas de seguridad.
CIR 12	Percepción errónea de capacidad legal para el tratamiento o cesión de datos personales, incluso entre responsables sin las formalidades que requiere la Ley.	Concientizar a las áreas responsables de SDP´s de la obligatoriedad de cumplir con el Principio de Responsabilidad.	-Elaborar el Documento de Seguridad, difundirlo en la SEDESOL. - Brindar capacitación y asesoría de acompañamiento de manera permanente. - Supervisar el cumplimiento de las medidas de seguridad.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

X. PLAN DE TRABAJO

Una vez que se han identificado los riesgos y se ha realizado el análisis de brecha en la que se han propuesto acciones concretas para reducir la probabilidad de que éstos se materialicen, entonces resulta necesario elaborar un plan de trabajo que permita lograr dicho objetivo, para ello es imprescindible contar con objetivos, metas, actividades, responsables y cronograma.

En consecuencia, se presenta como Anexo 1 el Plan de Trabajo en materia de Protección de Datos Personales de la SEDESOL.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

XI. MEDIDAS DE SEGURIDAD, MECANISOS DE MONITOREO Y REVISIÓN

Cuando se genera, procesa, transfiere y almacena información referente a una persona identificada o identificable, es necesario garantizar su debida protección, por ello se deben implementar controles que aseguren la integridad, confidencialidad y disponibilidad de la información de Datos Personales.

Como se dijo anteriormente, las medidas de seguridad físicas son:

- Cuerpo de vigilancia al acceso de cada edificio en el que se requiere identificación y conocer la persona que se visita, a quien se le solicita autorización para el ingreso.
- Libro de registro de visitas.
- Vigilantes en pisos que registran el nombre de la persona que ingresa (incluso siendo servidor público de la propia SEDESOL) y solicitan autorización del servidor público que es visitado.
- Equipo de videovigilancia.
- Los equipos de cómputo tienen asignado un usuario y cada uno la contraseña con la que pueden acceder al mismo.
- De acuerdo a los niveles de responsabilidad se asignan permisos de navegación y acceso a sitios de internet.
- Los equipos con inactividad se bloquean y para reiniciar se requiere introducir la contraseña cada que esto ocurre.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

Por otro lado, se presentan a continuación las medidas de seguridad que deberán observar las áreas que tienen a su cargo Sistemas de Datos Personales.

A) TRANSFERENCIA DE INFORMACIÓN

Cuando se realice la Transferencia de información deberán observarse las siguientes Medidas de seguridad.

- La transferencia de Datos Personales se debe realizar mediante acuerdos formales para el intercambio de información y, en su caso, de sistemas de información con otras entidades. Estos acuerdos serán de obligatorio cumplimiento.
- Los Datos Personales, sean información confidencial o sensible, contenidos en medios impresos deberá permanecer en espacios cerrados con llave, entregados en sobre cerrado o con embalaje con sellos de seguridad, entre otros mecanismos de seguridad requeridos o de acuerdo a la necesidad de la institución para proteger la información. Además, deberá señalarse que es responsabilidad de todo servidor público mantener la confidencialidad de la información relacionada con Datos Personales.
- Se debe hacer uso de la red institucional para realizar transferencia de información que contenga Datos Personales y SDP, para disminuir el riesgo de las transacciones mediante internet y evitar la transmisión incompleta, rutas equivocadas, alteración o divulgación.
- Para la transmisión de información que contenga Datos Personales y/o SDP mediante la Red de Datos SEDESOL, debe contar por lo menos con mecanismos de seguridad como:

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

- Firewall: administración de restricciones de acceso a aplicaciones, correo electrónico, puertos, sitios web, conexión con instituciones externas, entre otros.
- Directorio Activo: gestión sobre los permisos de la administración de los equipos, transferencia de archivos, entre otros.
- IPS: Detector y preventor de intrusos para captar ataques a la Red Institucional.
- Antispam: Permite realizar acciones de alertamiento y solución de posibles ataques por medio de correo electrónico.

- Si se cuenta con un proveedor de servicios (outsourcing) para un Centro de Datos, deberá contar por lo menos con las siguientes características:

RED LAN y CORE

- *El equipamiento que soporta la infraestructura de la red del Servicio Administrado de Centro de Datos, cuente con características de alta disponibilidad y redundancia en todos sus componentes, hardware y software son de última generación tecnológica, con soporte de mantenimiento.*
- *Cuente con listas de control de acceso y aplica dichas listas a tráfico de la red VLANS, previniendo el acceso de la gente o el flujo de los datos no permitidos en el equipo.*
- *Maneje un método seguro para la transferencia de los archivos imagen del switch hacia y desde el sistema a través de un canal encriptado usando Secure Shell.*
- *Maneje conexiones, telnet, configuración vía línea de comando y conexión SSH v2*
- *Cuente con la funcionalidad de obtener los registros del sistema (SYSLOG)*

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

- *Cuente con enlaces seguros(encriptados)*
- *El enlace debe ser monitoreado a través del protocolo SNMP, los paquetes viajan de forma cifrada y segura*
- *Cuente con un Centro de Operaciones de Seguridad por sus siglas en inglés (SOC) el cual consta de:*
    - *Analistas de seguridad calificados pantallas, consolas de dispositivos de seguridad administrados, estaciones de trabajo necesarias para monitorear y administrar la seguridad de los dispositivos involucrados en el servicio y cualquier otro elemento tecnológico necesario para cumplir con los niveles de servicios del Centro de Datos.*
        - *Administra y monitorea la operación de los equipos de seguridad*
        - *Administración de cambios de la configuración*
        - *Actualización de Software y controles*
        - *Administración de fallas técnicas con fabricantes*
        - *Administración de la configuración*
        - *Inventarios de equipos de seguridad administrados*
        - *Administración de configuraciones (bitácoras)*
        - *Administración de desempeño*

    - *Gestión de eventos de seguridad*
        - *Administración de las bitácoras de los controles*
        - *Investigación forense y recolección de evidencia digital.*
    - *Documentación de incidentes*
    - *El SOC cuenta con procedimientos y políticas de seguridad auditables que garantizan los mecanismos necesarios para*

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

asegurar e impedir acceso a usuarios no autorizados.

- *Cuente con DMZ que son zonas seguras(aisladas) donde radica la información*
- *Las medidas de seguridad que gestiona el SOC, permiten detectar amenazas de seguridad a la red, comportamientos de riesgo por parte de los usuarios, actividades relacionadas con problemas de desempeño de la red, violación a políticas y cambios no autorizados a la red.*
- *El Centro de Datos cuente con solución de Firewalls con el objetivo de filtrar el tráfico de la red mediante el bloqueo de accesos no autorizados al mismo.*

- Si se cuenta con un servicio *outsourcing* o tercero para la administración de la Red de la SEDESOL, se deberá solicitar que firme un acuerdo de confidencialidad que garantiza la total reserva de la información de Datos Personales, así como los alcances frente al tratamiento y divulgación de la información o en su caso se establecerá una cláusula de confidencialidad en el contrato de prestación de servicios que se firme para dicho efecto.
- Es importante mencionar que, si el usuario de Datos Personales realiza transferencia de información como parte de la operación diaria con áreas internas de la Institución o bien con entidades externas, el Responsable de la Información mediante un documento oficial (carta de confidencialidad) informará sus obligaciones y responsabilidades, con la finalidad de que el usuario pueda realizar las transferencias sin necesidad de informar al área Responsable de Servicios TIC, por tal motivo solo se notificara al Responsable de Servicios TIC y al Responsable de Seguridad de la Información cuando haga uso de la Red de Datos por primera vez.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

Procedimiento

La transferencia de información de datos personales de manera electrónica puede ser por dos medios, **medios físicos**: USB, discos duros, cd, memorias, entre otros y **medios electrónicos** como son: redes, acceso remoto, correo electrónico, mensajería electrónica, entre otros, por tal motivo es necesario asegurar la transmisión en sus dos formas, a continuación se describen los procesos de cómo realizar dicha transferencia de información.

Procedimiento para el intercambio de información digital en medio físico

1. Se debe contar con el convenio donde ambas partes (SEDESOL y Entidad externa) en base a las condiciones legales del intercambio de información vigentes, en dicho convenio se deben establecer las responsabilidades y obligaciones que se tienen para tratamiento de información, si no existe dicho documento no se podrá realizar ninguna transferencia de información que contenga datos personales. De igual forma se podrá transmitir la información con otros sujetos obligados, siempre y cuando la misma sea utilizada para el ejercicio de facultades propias de los mismos[6].

2. Una vez que se tenga el documento de convenio de intercambio de información o se haya corroborado que se transmite a otro sujeto obligado en ejercicio de sus facultades, el usuario de Datos Personales, inicia con el proceso de envío a la entidad de acuerdo a la vía elegida (que garanticen la confiabilidad de la información) de común acuerdo entre las partes: ejemplo mensajero oficial, servicio de mensajería externo, entre otras posibles. Se define un destinatario primario y otro secundario por si el mensajero no encuentra al primero.

[6] En términos de lo que disponen los Artículos 120 fracción IV y 117 fracción IV, de la Ley General de Transparencia y Acceso a la Información Pública y Ley Federal de Transparencia y Acceso a la Información Pública, respectivamente.

3. La información digital o electrónica debe enviarse de manera encriptada por lo menos con un nivel de protección medio o superior:

    1. Nivel de protección bajo, 128 bits de longitud;
    2. Nivel de protección medio, 512 bits de longitud; y
    3. Nivel de protección alto, 1024 bits.

4. El medio físico que contiene los datos personales de manera electrónica, viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo.

5. La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía y el mensajero entrega documento oficial de formalidad a la entrega, el cual como mínimo debe contar con:

    - Responsabilidades para controlar y notificar la transmisión y la recepción de información,
    - Responsabilidades en caso de incidentes de seguridad de la información.
    - Mencionar los mecanismos de seguridad con los que cuenta para su transmisión o traslado y cómo hacer para dar tratamiento a la información.

    En dicho documento se recupera el nombre, firma del destinatario, así como la fecha de recepción y un número de referencia que aparezca en tal identificación.

6. El mensajero no entrega el paquete si el destinatario no puede acreditar su identidad. En este caso, el mensajero devuelve el paquete al transmisor.

7. El transmisor verifica que el mensajero haya entregado el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente y se notifica a todos los involucrados (encargado y usuario de la información de Datos Personales,

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

así como DGTIC) para la atención y prevención del mal uso que pudieran hacer de dicha información.

8. El transmisor debe asegurar que el destinatario haya firmado el documento oficial de recepción de la información que contiene Datos Personales y así mismo debe registrar dicho envío en una bitácora de transmisión de información física.

9. El emisor se asegura que la información entregada este encriptada y que al desencriptarla cuente con la integridad de la información de Datos Personales, si detecta alguna anomalía deberá notificar al emisor de la información que fue recibida, entre ambas partes, deberán acordar la manera de verificar que la información esteintegra.

10. Fin del proceso.

La transmisión de Información que contiene Datos Personales y SDP de manera digital a través medios físicos, debe de ser aprobada por el Responsable, encargado (en su caso) y usuario de la información y, de considerarse necesario, solicitar acompañamiento de la DGTIC, para asegurar aún más su transferencia.

Procedimiento para el intercambio de información digital mediante medios electrónicos con otras entidades

1. El Responsable, solicita al Responsable de Datos personales mediante documento oficial realizar el intercambio de información con otra entidad.
2. El Responsable de la Información recibe solicitud y analiza si es posible realizar la transferencia de información con Datos Personales, si el Responsable de la Información autoriza, notifica mediante documento oficial la solicitud aprobada para realizar dicha transferencia, si la respuesta es negativa también lo informa

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

mediante documento oficial, explicando el motivo por el cual no puede realizar dicho intercambio.

3. Si el Responsable recibe aprobación por parte del Responsable de Datos Personales, realiza el convenio de intercambio con la otra entidad, debidamente aprobado y firmado por todos los involucrados.
4. Una vez que el Responsable cuenta con el convenio de intercambio de información, solicita a la DGTIC llevar a cabo el intercambio de información con otra entidad mediante la red de datos institucional a través de documento oficial y formato de solicitud de servicio, indicando:
    - Características de la información
    - Volumen de la información
    - Dependencia a donde será enviada
    - Mecanismo de transferencia (correo electrónico, Acceso remoto VPN, Red inalámbrica WIFI, Telnet, entre otros)
    - IP de donde será transmitida la información
    - En todo caso la IP o ruta donde será transmitida la información

5. La DGTIC recibe solicitud de intercambio de información por parte del Responsable y analiza dicha solicitud.

6. Si la solicitud no es aprobada por la DGTIC, envía notificación mediante documento oficial, explicando motivos por los cuales no será posible realizar el intercambio y si fuera el caso, posibles alternativas para realizarlo de otra manera, si la solicitud es aprobada, la DGTIC notifica mediante documento oficial las instrucciones para realizar el intercambio de información y estableciendo fecha y hora para trabajar en conjunto para dicha actividad.

7. El Responsable recibe respuesta a la solicitud aprobada y de acuerdo a las instrucciones de la DGTIC, deberá ponerse en contacto con la DGTIC, para el acompañamiento con el intercambio de información.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

8. Una vez finalizada la solicitud de intercambio de información, se firma reporte de actividad en común acuerdo por ambas partes (DGTIC y Responsable).

9. Fin del proceso

Procedimiento para el intercambio de información digital mediante medios electrónicos en la red institucional

Si se requiere transmitir información que contiene Datos Personales dentro de la Red de datos SEDESOL, es necesario hacer de conocimiento a la DGTIC para establecer mecanismos de seguridad, si fuera necesario dicha transferencia, a continuación, se describe el proceso de como asignar un servicio para conexión a la red de datos SEDESOL:

1. El Responsable del Sistema de Datos personales recibe la petición, mediante documento oficial, de realizar el intercambio con otra unidad administrativa de la SEDESOL.
2. El Responsable de la Información recibe solicitud y analiza si es posible realizar la transferencia de información con Datos Personales; si el Responsable de la Información autoriza, notifica mediante documento oficial la solicitud aprobada para realizar dicha transferencia; si la respuesta es negativa también lo informa mediante documento oficial, explicando el motivo por el cual no puede realizar dicho intercambio.
3. En caso de que el requirente se trate de otro sujeto obligado, el Responsable de Datos Personales realiza el convenio de intercambio con la otra unidad administrativa, debidamente aprobado y firmado por todos los involucrados o revisa que la información se vaya a utilizar para el ejercicio de las facultades del área que la solicita.
4. Una vez que el Responsable cuenta con el convenio o acuerdo de intercambio de información, solicita a la DGTIC llevar a cabo la conexión a la red

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

institucional, para que mediante la misma se realice la transferencia de información con Datos Personales, esta solicitud se hace a través de documento oficial y formato de solicitud, indicando:

- Características de la información
- Volumen de la información
- Área donde se recibirá la información.
- Mecanismo de transferencia (correo electrónico, Acceso remoto VPN, Red inalámbrica WIFI, Telnet, entre otros)
- IP de donde será transmitida la información
- En todo caso la IP o ruta donde será transmitida la información

5. La DGTIC recibe solicitud de intercambio de información por parte del Responsable y analiza dicha solicitud.

6. Si la solicitud no es aprobada por la DGTIC, envía notificación mediante documento oficial, explicando motivos por los cuales no será posible realizar el intercambio y si fuera el caso, posibles alternativas para realizarlo de otra manera, si la solicitud es aprobada, la DGTIC notifica mediante documento oficial las instrucciones para realizar el intercambio de información y estableciendo fecha y hora para trabajar en conjunto para dicha actividad.

7. El Responsable recibe respuesta a la solicitud aprobada y de acuerdo a las instrucciones, deberá ponerse en contacto con la DGTIC, para el acompañamiento con el intercambio de información.

8. Una vez finalizada la solicitud de intercambio de información, se firma reporte de actividad en común acuerdo por ambas partes (DGTIC y Responsable).

9. Fin del proceso.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

B) ASIGNACIÓN Y BAJA DE CLAVE DE ACCESO

Si se genera, procesa, transmite y almacena información que contiene Datos Personales y SDP es necesario contar con controles para evitar que personas no autorizadas accedan a dicha información, a continuación, se muestran las medidas mínimas de seguridad para el uso de claves y contraseñas.

Medidas de seguridad

Los Sistemas de Datos Personales, deben contar con niveles de acceso como mínimo:

- **Nivel de Administrador**. Sirve para gestionar los usuarios de la cuenta (agregar y suprimir usuarios, y asignar permisos). Este permiso excluye los permisos de edición y de colaboración. de la información no restringida o reservada.

- **Nivel de escritura**. Sirve para realizar funciones administrativas y relacionadas con los informes (como agregar, editar o suprimir cuentas, propiedades, vistas, filtros, objetivos, etc., pero sin gestionar usuarios),

- **Nivel de lectura**. Incluye el permiso Leer y analizar.

Los activos que es necesario contar con control de acceso son:

- Sistemas de Información
- Aplicativos (Sistema operativo, bases de datos, entre otros)
- Equipo de cómputo
- Red de datos (wifi)
- Impresoras
- Accesos remotos
- Entre otros

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

Todos los servidores públicos de SEDESOL, que hagan uso de información con Datos Personales, requieren de manera obligatoria la asignación de un usuario y una contraseña para poder acceder a la misma.

Cada usuario se responsabilizará por el mecanismo de acceso lógico asignado, esto es su identificador de usuario y contraseña necesarios para acceder a la información, además es responsabilidad de cada usuario la confidencialidad de los mismos.

El acceso a la información al Sistema de Datos Personales, se otorga en base a las funciones del usuario, se deberán otorgar los permisos mínimos necesarios para el desempeño del cargo o rol.

El Administrador de contraseñas de los sistemas de información o aplicativos deberá llevar un control de altas y bajas de usuarios para monitorear que todas las cuentas que estén vigentes son las que están en operación y evitar que se tengan cuentas sin utilizar o bien que ya no deben existir. Para ello los usuarios deberán observar lo siguiente:

- La cuenta de usuario se protege mediante una contraseña.
- La cuenta de usuario se protegerá mediante una contraseña. La contraseña asociada a la cuenta de usuario, deberá seguir los Criterios para la Construcción de Contraseñas.

Una contraseña segura deberá cumplir con las siguientes características:

- Longitud mínima de 8 caracteres.
- Contener al menos:

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

- Un carácter numérico.
- Un carácter especial si el sistema lo permite (_.-¿?¡#$%&/).
- Una letra mayúscula.
- Una letra minúscula.

- Elegir una contraseña que pueda recordar fácilmente, por ejemplo, utilizar el título de una canción o película y transformarlo en una contraseña segura, ejemplo:
  - “La vida es bella” → 1aViDaEsBe11a
- Se recomienda alternar letras mayúsculas y minúsculas.
- Cambiar la contraseña por lo menos una vez cada seis meses. No utilizar consecutivos al realizar el cambio, ej. “sedesol2016” por “sedesol2017”.
- No utilizar datos personales como fechas de nacimiento propias o de familiares, números de teléfono, RFC, nombres de mascotas, etc.
- Evitar utilizar la misma contraseña para diferentes sistemas.
- No utilizar secuencias básicas de teclado: “qwerty”, “asdfghjk” o las típicas de numeración “12345678”, “98765432”.
- No repetir caracteres: “11112222”.
- Evitar utilizar solamente números o solamente letras mayúsculas o minúsculas.
- No utilizar como contraseña, ni contener, el nombre de usuario.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

- No utilizar datos relacionados con el usuario que sean fácil de deducir, como apodos, cantante o actor favorito, color favorito, etc.
- No escribir ni reflejar las contraseñas en documentos o lugares donde sea de fácil acceso para otras personas, tampoco se deben guardar en notas o documentos dentro de la computadora.
- No enviar nunca la contraseña por correo electrónico o mensaje de texto.
- No utilizar las contraseñas asociadas a sistemas de información de la SEDESOL en ordenadores de terceros o públicos de los cuales se desconozca su nivel de seguridad.
- Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes o por el personal de DGTIC.
- Mantener las contraseñas en secreto y no compartirlas con nadie.

Procedimiento para asignar un usuario y contraseña a un sistema de información y/o aplicativos.

1. El Responsable realiza un análisis de cuál es el perfil que requiere el nuevo Usuario de Datos Personales de acuerdo al rol y funciones para el SDP.
2. Una vez definido el perfil, el Responsable solicita a la DGTIC mediante documento oficial y formato de solicitud de servicio, el alta de usuario y contraseña para un nuevo Usuario de Datos Personales a sistema de información o aplicativo.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

3. La DGTIC, recibe solicitud y formato de alta de usuario y la analiza, si la solicitud no es aprobada, envía documento oficial donde notifica que la solicitud no es viable explicando los motivos por la cual no es posible la asignación.

4. Si la solicitud es aprobada, la DGTIC solicita al proveedor de servicios de Centro de Datos realice el alta de usuario, una vez que el proveedor realiza el alta de usuario envía usuario y contraseña y pide a DGTIC que verifique si el usuario puede ingresar al sistema o aplicativo.

5. La DGTIC mediante documento oficial notifica al Responsable de la información que la solicitud es aprobada, enviando usuario y contraseña mediante correo electrónico.

6. En Responsable, envía usuario y contraseña al Usuario de Datos personales para que verifique si la contraseña es correcta, si la contraseña no es correcta pide a DGTIC mediante llamada telefónica apoye para que se revise el alta del usuario y contraseña. DGTIC solicita al proveedor del Centro de Datos revise la configuración del usuario y contraseña, este paso se repetirá hasta que la contraseña este correcta, una vez que el usuario valida la entrada al sistema de información o aplicativo, notifica a DGTIC el acceso correcto.

7. Una vez que el usuario y contraseña están correctos la DGTIC notifica al proveedor que el usuario y contraseña son correctos y se firma formato de solicitud entre el Responsable y la DGTIC de común acuerdo que el servicio ha finalizado correctamente.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

En el caso de **la modificación o baja de usuarios, contraseñas, perfiles** de usuario o roles, el procedimiento será el mismo al anterior especificando la baja del usuario o cambio que se requiere.

C) RESPALDO DE INFORMACIÓN

La información que contiene Datos Personales, es información sensible que debe estar protegida contra diversas amenazas como son daño, destrucción, robo, entre otros, por lo que es necesario respaldar la información y mecanismos de recuperación por si alguna de las amenazas pudiera afectar y estar preparados para ciertos incidentes y dar continuidad operativa de los procesos y servicios, dando cumplimiento a la misión de la SEDESOL.

El respaldo de información corresponde a la copia de datos de un dispositivo primario en uno o varios dispositivos secundarios, ejemplo: en el caso de que el primer dispositivo sufra un desperfecto electromecánico o un error en su estructura lógica, sea posible disponer de la mayor parte de la información necesaria para la continuidad operacional y evitar pérdida generalizada de datos.

Medidas de seguridad

- El Encargado de la Información de Datos Personales, asegura que la información que contienen Datos Personales y SDP, cuente con respaldos de información de los equipos donde está contenida dicha información, lo anterior de acuerdo a la necesidad y criticidad de Datos Personales
- Se debe respaldar la información que contenga Datos Personales, por lo menos en los siguientes activos:
    - El SDP
    - Aplicativos (Sistemas Operativos, Bases de Datos)

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

- Códigos Fuentes
- Correos electrónicos
- Repositorios de información
- Documentos digitales que deriven del SDP o que contengan Datos Personales.
- Entre otros.

Frecuencia de respaldo

- La frecuencia dependerá de la criticidad que tenga la información con Datos Personales, entre el Responsable, el encargado y usuario tendrán que decidir que criticidad tienen dichos Datos, por lo que a continuación se listan los periodos en que pueden realizarse los respaldos:
  - Incremental.- 7 días
  - Full semanal.- 4 a 5 días de la semana
  - Full mensual.- 3 meses
  - Full anual.- 1 año

Medio de respaldo

Los medios de respaldo para los servidores son:

- Pueden ser servidores de grandes capacidades.
- Equipos con arreglos de discos duros para almacenamiento de información.
- Discos duros externos.
- USB, entre otros.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

- Los respaldos que se realizan con mayor frecuencia serían los indicados para una criticidad más alta de información de Datos Personales, es importante mencionar que es necesario determinar la información de prioridad y la que no tiene prioridad, debido a que los respaldos de información son espacios en equipos robustos de información y que almacenan información que es necesario ir depurando de lo contrario dichos equipos podrían saturarse impidiendo el almacenamiento de la información y generando costos adicionales.
- Los Usuarios de Datos Personales deberán respaldar su información de sus equipos de cómputo personal institucional, por lo menos una vez a la semana o bien de acuerdo a la criticidad de la información que maneje, es importante mencionar que el medio que utilice para dicho respaldo no podrá salir de la Institución al menos que se lleve a cabo una transmisión de información y sea aprobada por escrito por el Responsable de la información.
- La DGTIC, debe informar al Usuario de Datos Personales, la capacidad del equipo de almacenamiento de información de Datos Personales, para que lleven un control de sus respaldos de información y evitar colapsar el equipo de respaldo y por ende pérdida de información.
- Si el Responsable o el usuario de Datos Personales son los administradores del SDP y por ende de la gestión de respaldos, deberán velar por una adecuada gestión de los respaldos de información, así como de los activos (servidores, NAS, discos duros, USB) que la contienen, evitando incidentes de la información de Datos Personales.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

Procedimiento para solicitar se integre configuración de respaldo de información a sistema de información o aplicativo

1. El Responsable, solicita a la DGTIC mediante documento oficial y formato de solicitud de servicio respaldo de información.

2. La DGTIC, recibe solicitud y formato respaldo de información, si la solicitud no es aprobada, envía documento oficial donde notifica que la solicitud no es viable explicando los motivos por la cual no es posible la asignación.

3. Si la solicitud es aprobada la DGTIC, solicita al proveedor de servicios de Centro de Datos cotice el servicio de respaldo de información, el proveedor envía cotización del servicio a ejecutar.

4. DGTIC envía cotización de servicio al Responsable por correo electrónico, para su aprobación del servicio.

5. Si el Responsable, no aprueba la ejecución, notifica a DGTIC mediante correo electrónico explicando el por qué no se llevará a cabo el servicio, si la solicitud es aprobada, notifica a DGTIC mediante correo electrónico, DGTIC recibe la aprobación y solicita al proveedor se ejecute el servicio de respaldo de información de sistema de información o aplicativo

6. Cuando el proveedor finaliza la configuración notifica a DGTIC que la configuración ya fue concluida, DGTIC notifica al Responsable que la solicitud ha finalizado y se firma formato de solicitud y termino del servicio mediante común acuerdo.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

Procedimiento de Recuperación de la información

1. El Responsable, solicita a la DGTIC mediante documento oficial y formato de solicitud de servicio de recuperación de respaldo de información.

2. La DGTIC, recibe solicitud y formato de recuperación de respaldo de información, si la solicitud no es aprobada, envía documento oficial donde notifica que la solicitud no es viable explicando los motivos por la cual no es posible la asignación.

3. Si la solicitud es aprobada la DGTIC, solicita al proveedor de servicios de Centro de Datos cotice el servicio de recuperación de respaldo de información, el proveedor envía cotización del servicio a ejecutar.

4. DGTIC envía cotización de servicio al Responsable por correo electrónico, para su aprobación del servicio.

5. Si el Responsable, no aprueba la ejecución, notifica a DGTIC mediante correo electrónico explicando el por qué no se llevará a cabo el servicio, si la solicitud es aprobada, notifica a DGTIC mediante correo electrónico.

6. DGTIC recibe la aprobación y solicita al proveedor de Centro de Datos, se ejecute el servicio de recuperación de respaldo del sistema de información o aplicativo.

7. Cuando el proveedor finaliza la recuperación del respaldo notifica a DGTIC que el respaldo ya fue recuperado y que está contenido en la ruta que se solicitó se almacenara.

8. DGTIC notifica al Responsable y usuario de Datos Personales que ya se cuenta con el respaldo recuperado para que verifique si el respaldo está completo o bien si es posible ejecutarlo

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

9. El usuario de Datos Personales verifica su respaldo recuperado, si el respaldo no funciona o marca algún error, notifica de inmediato a la DGTIC, se revisa con el usuario la recuperación del respaldo para verificar si es algún error del sistema o bien del respaldo, cuando finalizan el análisis, si determinan que es un problema de sistema verifican hasta resolver, si es un problema del archivo de respaldo, se solicita apoyo del proveedor para revisar o ejecutar nuevamente la recuperación del archivo de respaldo, esta actividad se repite hasta solucionar error.

10. Cuando el Responsable aprueba que el archivo se ha ejecutado correctamente, DGTIC notica al proveedor que el archivo fue ejecutado con éxito y así mismo, se firma formato de solicitud y termino del servicio mediante común acuerdo.

D) BITÁCORAS DE INFORMACIÓN

Durante la generación, procesamiento, transferencia y almacenamiento de Datos Personales se ven expuestos a diversos riesgos, como son robo de información, destrucción de información, acceso a personal no autorizado, entre otros. Dichos riesgos son minimizados mediante la aplicación de medidas o controles administrativos, físicos y técnicos, uno de éstos es el de monitoreo mediante bitácoras de información donde se registra la actividad que es realizada en los SDP y permite detectar incidentes de seguridad o para auditar la actividad anómala en el Sistema.

Medidas de seguridad

Las bitácoras de información cuentan con ciertas características y dependerá de que información se requiere monitorear:

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

Por su orientación

- Aplicación: indican los sucesos que están activados para registrarse en una aplicación.
- Seguridad: orientadas a dar información de seguridad.
- Sistema: registran actividades del sistema (usualmente donde reside la aplicación).

Por la forma en que se generan

- Archivos: algunos sistemas generan bitácoras en archivos (tipo FILE). Aquí se recolecta el archivo para procesar las bitácoras desde ahí.
- Base de datos: varias aplicaciones, en especial las desarrolladas en casa, generan bitácoras que se almacenan en bases de datos.
- Windows Event Log: bitácora de eventos del sistema operativo de Microsoft.
- Check Point Log: bitácora específica de Check Point extraíble mediante conexiones propietarias LEA.

Elementos que con que debe contar una bitácora de manera digital

1. Fecha de ingreso.
2. Hora de ingreso.
3. Direcciones IP origen y destino.
4. Dirección IP que genera la bitácora.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

5. Nombre de usuario.

6. Actividades realizadas en sistema (detección de errores).

7. Hora de salida.

- El Responsable y usuario de Datos Personales, deben establecer un plan de bitácoras del SDP y los activos que contengan la información con Datos Personales, por lo que solicitará a la DGTIC asesoría, para establecer el tipo de bitácora conveniente para el SDP, todo dependerá de la criticidad de la información, capacidad de los activos que contienen la información (hardware y software) y los incidentes que han ocurrido en su SDP.
- El Responsable y usuario de Datos Personales deberán asegurar que las bitácoras de información se almacenen por lo menos de 2 meses y que se hagan respaldos de dichas bitácoras.
- Es importante mencionar que las bitácoras generan grandes volúmenes de información y será necesario monitorear y administrar los equipos donde se almacenaran las bitácoras y evitar colapsar dichos equipos por falta de espacio o memoria.

Procedimiento para solicitar se integre configuración de bitácoras de información a sistema de información o aplicativo

1. El Responsable, solicita a la DGTIC mediante documento oficial y formato de solicitud de servicio de bitácoras de información a sistema de información o aplicativo.

2. La DGTIC, recibe solicitud y formato respaldo de información, si la solicitud no es aprobada, envía documento oficial donde notifica que la solicitud no es viable explicando los motivos por la cual no es posible la asignación.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

3. Si la solicitud es aprobada la DGTIC, solicita al proveedor de servicios de Centro de Datos cotice el servicio de bitácora de información, el proveedor envía cotización del servicio a ejecutar.

4. DGTIC envía cotización de servicio al Responsable por correo electrónico, para su aprobación del servicio.

5. Si el Responsable, no aprueba la ejecución, notifica a DGTIC mediante correo electrónico explicando el por qué no se llevará a cabo el servicio, si la solicitud es aprobada, notifica a DGTIC mediante correo electrónico.

6. DGTIC recibe la aprobación y solicita al proveedor se ejecute el servicio de bitácora de información de sistema de información o aplicativo.

7. Cuando el proveedor finaliza la configuración notifica a DGTIC que la configuración ya fue concluida, DGTIC notifica al Responsable que la solicitud ha finalizado y se firma formato de solicitud y termino del servicio mediante común acuerdo.

Es importante mencionar que cada aplicativo cuenta con su propio formato de bitácora por lo que el proceso para revisar es diferente, se solicitará asesoría de DGTIC para identificar su localización y revisión del formato.

E) RESPUESTA A INCIDENTES

Durante el generación, procesamiento, transferencia y almacenamiento de Datos Personales se encuentra expuesta a diversos riesgos, los cuales son minimizados mediante la aplicación de medidas o controles administrativos, físicos y técnicos. Por tal motivo es necesario contar con un registro de incidentes para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

Medidas de seguridad

Diversos activos de información deberán ser protegidos ante incidentes, amenazas y/o debilidades:

- Servidores.
- Equipos de conectividad (Firewall, Routers, Switches, Access points.).
- Enlaces de telecomunicaciones (Internet, MPLS, Telefonía)
- Computadores personales.
- Impresoras.
- Sistema de control de acceso y cámaras de video vigilancia.
- Central telefónica y Equipos telefónicos.
- Sistemas de información, aplicaciones y software en general.
- Cualquier otro servicio computacional entregado por la SEDESOL

Se identifican los siguientes tipos de incidentes, que pueden representar una amenaza para la seguridad de la información:

- Incendio o inundación en la sala de servidores.
- Robo de computadores personales.
- Robo de información electrónica.
- Ingreso de personal no autorizado en la sala de servidores o estaciones de trabajo
- Corte eléctrico o defectos en el sistema eléctrico.
- Hacking y técnicas de suplantación.
- Virus informáticos y spyware.
- No disponibilidad de Portal institucional y sistemas de información.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

Procedimiento para registrar un incidente

- Ante la ocurrencia de incidentes o la detección de amenazas y/o debilidades que pudiesen comprometer la seguridad de la información de los Datos Personales y de los activos que la contienen el Responsable, el Encargado y el usuario de la Información de Datos Personales, según sea el caso, deberán dar aviso inmediato al Responsable de Seguridad de la Información y al Responsable de Servicios de la DGTIC, incluso durante días no hábiles, mediante llamada telefónica o mediante correo electrónico.
- Será obligación del Responsable de Servicios de la DGTIC, entregar al Responsable, Encargado y al usuario el nivel de atención para incidentes de los servicios de TIC, ya que dependiendo la complejidad del incidente es como se dará la atención.
- Solo en el caso de que fuera algo que atentará en contra de información de Datos Personales y pudiera afectar a los Titulares, se notificará directamente al Responsable de la Seguridad de la Información y al Responsable de Servicios de la DGTIC, como se menciona en el punto anterior.
- La primer vía formal de reporte de incidentes o amenazas será mediante el **envío de correo electrónico** a las siguientes cuentas: **mesadeayuda@ste.mexico** colocando en el asunto del correo la frase “Incidente de seguridad de información” u otra similar que permita reconocer la situación rápidamente. Se deberá ser lo más claro y preciso en especificar el incidente o amenaza y a que recursos tecnológicos podría estar afectando y los datos de la persona que reporta: nombre, unidad responsable, inmueble, extensión telefónica, piso donde se ubica, posteriormente levantaran un ticket del servicio y posteriormente un ingeniero se comunicará para dar atención hasta concluir con el servicio.
- El siguiente medio para reportar incidentes es mediante llamada telefónica a la **mesa de ayuda, en la extensión 44500,** donde solicitarán los datos

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

necesarios para generar el ticket de atención al incidente, posteriormente un ingeniero se comunicará para data atención hasta concluir con el servicio.

- Una vez recibido el incidente mediante correo electrónico, llamado telefónico o contacto personal, un ingeniero especialista toma conocimiento y asigna el ticket a un especialista en la materia según la clasificación de servicios de TIC, quien deberá iniciar una investigación.
- Detectada las causas del problema y los elementos afectados, se informará al Jefe del área de atención sobre el plan de solución, tiempos involucrados y recursos necesarios, dependiendo del grado de complejidad y magnitud del problema, quien deberá realizar las gestiones correspondientes, incluyendo la comunicación al Jefe de área del Servicio y al usuario.
- El Responsable de Servicios de TIC, verifica que exista un registro actualizado de incidentes y/o amenazas, incluyendo todas las acciones o medidas que se implementen para solucionarlos, ya sea de forma total o parcial.
- Si el incidente atenta contra la Información que contiene Datos Personales se deberá enviar un informe tanto de la trazabilidad de atención al incidente como de la solución a dicho incidente, con copia al Comité de Transparencia para que tome las medidas que resulten pertinentes de acuerdo al caso concreto.

F) ACTUALIZACIÓN DE SISTEMAS DE INFORMACIÓN

La información que contiene Datos Personales, por la sensibilidad que maneja requiere de transacciones de altas, bajas, cambios o bien transferencias debidamente autorizadas por parte de quien tenga atribuciones para ello, ya que se puede correr el riesgo de que existan modificaciones no autorizadas a dicha información, por tal motivo es necesario llevar a cabo un plan o control de cambios del procesamiento de la información y con ello asegurar la confidencialidad, disponibilidad e integridad de la información.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

Medidas de seguridad

- Para identificar los cambios que se realizan en cada SDP o aplicativo, es necesario configurar una aplicación o realizar alguna configuración en dicho sistema para obtener una trazabilidad de las actividades que se realizan en el sistema.
- Es necesario contar con un control de cambios entre los diversos usuarios del SDP, por lo que es necesario configurar una bitácora del SDP o aplicativo.
- Es necesario contar con un control de cambios de los equipos que hacen uso los Usuarios de Datos Personales.
- Los responsables y usuarios se coordinarán con la DGTIC en caso de que se deba realizar alguna de las actualizaciones mencionadas en este apartado.

G) CANCELACIÓN DE LOS SISTEMAS DE DATOS PERSONALES

La cancelación da lugar al bloqueo de los datos, esto es, el periodo en el que se conservarán los datos para efectos de responsabilidades, el cual será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento, en términos de la normatividad aplicable y, cumplido este plazo, deberá procederse a la supresión del dato que implica el borrado físico del mismo.

Bajo este contexto, **la cancelación no supone automáticamente la supresión o borrado físico de los datos, sino que se debe determinar un período o fase previa de bloqueo de los datos**, en el cual no se podrá disponer de tales datos en la misma medida en que podría hacerse por la unidad administrativa de estar en operación el Sistema.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

La cancelación de sistemas de datos personales debe considerar lo establecido en los Lineamientos de archivos y en concordancia con ello, se debe establecer un procedimiento de cancelación el cual deberá proponerse por parte del Responsable de la información.

En ese sentido se debe considerar lo establecido en el Primero de los Lineamientos de archivos que señala criterios de organización y conservación de la documentación de las dependencias y entidades de la APF con el objeto de conservar íntegros y disponibles los documentos para permitir y facilitar el acceso a la información que contengan.

Dichos Lineamientos de archivo establecen que se debe incluir la siguiente información en el Catálogo de disposición documental: -un registro general y sistemático que establece los siguientes valores documentales-:

A. los plazos de conservación;

B. la vigencia documental;

C. la clasificación de reserva o confidencialidad, y

D. el destino final de los documentos.

El Decimoquinto de los Lineamientos dispone que cuando se pretende dar de baja un sistema de datos personales se debe verificar en primer lugar, si el mismo tiene valores históricos, científicos, estadísticos o contables. En caso de que contenga dichos valores, los datos personales serán objeto de transferencias secundarias, de conformidad con lo establecido por los catálogos de disposición documental a que se refieren los "Lineamientos Generales para la organización y conservación de archivos de las dependencias y entidades de la Administración Pública Federal" -Lineamientos de Archivos-.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

Dado lo anterior, dicho Catálogo de disposición documental y el procedimiento de cancelación de un sistema deben atender al valor documental de la información contenida en el mismo, de conformidad con los criterios establecidos por la Coordinación de Archivos[7] en consideración a la posible consulta que de los mismos se requiriera o a cualquier otra implicación jurídica que pudiera existir en razón de la normatividad aplicable. Lo anterior es así, en virtud de que la organización de los archivos de las dependencias y entidades en los que se incluyen los sistemas de datos personales debe asegurar la disponibilidad, localización y conservación de los documentos de archivo que se posean.

1. Para iniciar el procedimiento de cancelación de un sistema de Datos personales, se deberá enviar, en su caso, solicitud al Responsable de Datos Personales con los siguientes datos:

- **Datos del sistema que será cancelado:**
    - Denominación
    - Folio del Sistema de Datos Personales
    - Motivo de la cancelación
- **Plazos y condiciones para el bloqueo del sistema:**
    - ***[Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad específica aplicable. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo]***

[7] Dependiente de la Dirección General de Recursos Materiales, que se encuentra adscrita a la Oficialía Mayor.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

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

2. Si la solicitud es aprobada, el Responsable de la Información deberá requerir mediante documento oficial a la DGTIC emita un análisis del medio en donde pueda resguardar la información a bloquear y la forma en que puede ser encriptada de acuerdo a la criticidad y volumen de la información a bloquear.
3. La DGTIC recibe solicitud y analiza.
4. La DGTIC, envía mediante documento oficial el análisis para resguardar la información y para aprobación del resguardo de información.
5. Si el Responsable no aprueba la solicitud deberá notificar por escrito el motivo por el cual no requiere el servicio, si la solicitud es aprobada, envía mediante documento oficial la aprobación para la ejecución del servicio.
6. DGTIC recibe la aprobación del servicio de resguardo de información y solicita al proveedor de centro de datos la cotización del servicio de resguardo de información.
7. El proveedor ejecuta servicio y notifica a DGTIC una vez que el servicio ha finalizado.
8. DGTIC, notifica al Responsable que la información ha sido resguardada y se firma formato de común acuerdo del servicio ha finalizado.
9. Cuando se cumpla el termino de resguardo de información, el Responsable envía solicitud a la DGTIC, para iniciar el proceso de borrado de información.
10. La DGTIC recibe solicitud y es enviada al proveedor de Datos Personales para iniciar con el proceso de borrado seguro.
11. Cuando e proveedor finaliza el servicio notifica a DGTIC.
12. DGTIC notifica a Responsable que el servicio ha finalizado y firman formato de común acuerdo de término del servicio.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

XII. PROGRAMA GENERAL DE CAPACITACIÓN

A efecto de promover una Cultura de Protección de Datos al interior de la SEDESOL se ha considerado la realización una campaña de promoción entre los Responsables y Usuarios de los Sistemas de Datos Personales. Esta difusión incluirá el diseño de un taller denominado: “Introducción al Documento de Seguridad” para concientizar a los servidores públicos de la importancia de cumplir con los Principios establecidos en la Ley General de Protección de Datos Personales y de observar las medidas de seguridad para su protección.

De igual manera, con la publicación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados resulta necesario la capacitación en dicha normatividad, para ello el 19 de abril del año en curso se remitió al INAI el Programa Anual de Capacitación (PAC) en el que se incluyó el curso denominado “Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados”, mismo que será tomado por los responsables y usuarios de los Sistemas de Datos Personales de acuerdo a lo proyectado en dicho documento. El PAC se exhibe como Anexo 2 de este documento.

Adicionalmente, la Unidad de Transparencia de la SEDESOL ha solicitado, al área de capacitación del INAI, la impartición de por lo menos un curso de protección de datos personales por parte del área especializada de dicho Instituto. Está pendiente la respuesta a la petición para coordinar las acciones necesarias para llevar a cabo dicha capacitación.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

XIII. ANEXOS

Anexo 1. Plan de Trabajo en materia de Protección de Datos Personales de la SEDESOL.

Anexo 2. Plan Anual de Capacitación de la SEDESOL.

Anexo 3. Fuentes de consulta.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol

El presente Documento de Seguridad fue elaborado por un grupo de trabajo coordinado por Javier Ortiz Moreno y en el que participaron los siguientes servidores públicos:

Por la Dirección General de Tecnologías de la Información y Comunicaciones:

Ignacio Alberto Bravo González. Dirección General Adjunta de Proyectos de Desarrollo de Soluciones Tecnológicas.

Laura Román Vergara. Líder de Proyecto.

Pedro Rincón Rivas. Líder de Proyecto.

Por la Dirección General de Geostadística y Padrones de Beneficiarios:

Joann Stefany Gil Ramos. Subdirectora de Vinculación Operativa.

Por la Unidad del Abogado General y Comisionado para la Transparencia:

Javier Ortiz Moreno. Director de Análisis e Información Institucional.

Ilse Lizeth Andrade Escamilla. Subdirectora de Monitoreo de Acciones de Transparencia.

Renata Yunuen Ubriaco Contreras. Subdirectora de Instrumentación de Programas Concertados.

Av. Paseo de la Reforma 116, Col. Juárez, Delegación Cuauhtémoc, CP 06600, Ciudad de México
Tel. (55) 5328 5000 ext. 51607 www.gob.mx/sedesol