FIDEICOMISO PARA LA ADMINISTRACIÓN DEL PROGRAMA DE DESARROLLO FORESTAL DEL ESTADO DE JALISCO

DOCUMENTO DE SEGURIDAD

COMITÉ DE TRANSPARENCIA

El presente documento contiene las disposiciones en materia de protección de datos personales de las unidades administrativas que forman parte de este Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco.

2019

Documento de Seguridad del Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco

Contenido

Glosario

Ley	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios
FIPRODEFO	Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco
ITEI	Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco
Derechos Arco	Derecho a la Actualización, Rectificación, Cancelación y Oposición de los datos personales.

Introducción

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios tiene por objeto establecer las bases, principios, obligaciones y procedimientos para garantizar el derecho que tiene toda persona al debido tratamiento y protección de sus datos personales. Así como a garantizar el derecho de acceso, rectificación, cancelación y oposición de los mismos.

Teniendo como base la normativa de esta Ley y de conformidad con su artículo 3 fracción XIV y los artículos contenidos dentro del Título Segundo Capítulo II (art 30 al 44); así como la Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales del 2015, emitida por el Instituto Nacional del Transparencia y Protección de Datos Personales Federal de Acceso a la Información; al igual que la Guía para elaborar un Documento de Seguridad/Formato guía para sujetos obligados del año 2018, del ITEI

A partir de la publicación de la Ley, el Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco por conducto del titular de su Unidad de Transparencia, con la participación de las Unidades Administrativas generadoras de información, se establecieron las acciones conducentes con la finalidad de establecer los soportes para la realización del presente documento.

Una de las acciones primordiales fue la elaboración de un Inventario de Datos Personales que permite la identificación básica de información y el tratamiento al que son sometidos por cada una de las Unidades Administrativas y sensibilizar a estas sobre la importancia del resguardo de datos personales.

El presente documento permite identificar los datos personales recabados por este FIPRODEFO y en consecuencia la creación del Sistema de Tratamiento de Datos Personales sobre los mismos.

Desde la publicación de la multicitada Ley, la Unidad de Transparencia ha realizado capacitaciones especializadas en materia de protección de datos personales con la finalidad de enseñar, habilitar e instruir a los trabajadores sobre el tratamiento lícito y adecuado de los datos personales.

Para la realización del Inventario de Datos Personales, se realizó un cuestionario en la materia de cada una de sus áreas a todas las Unidades Administrativas; mediante este estudio se detectaron los datos personales recabados por cada una de ellas, así como las medidas de seguridad con las que se contaban dentro del FIPRODEFO e identificar los posibles riesgos.

A partir de la creación del Inventario de Datos Personales, capacitaciones y diversas sesiones con las unidades administrativas, se recabó la información necesaria para generar cada una de las partes que integran el presente Documento de Seguridad; en donde el objetivo primordial es la protección y adecuado tratamiento de los datos personales custodiados por este FIPRODEFO.

El Documento de Seguridad que se leerá a continuación se rige por los principios que marca la Ley, primordialmente por lo dictado en su numeral 2.

Objetivo

Este documento es de orden obligatorio y su objetivo es asegurar la integridad, la confidencialidad y disponibilidad de los datos e información personal que se encuentran en posesión del Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco, en su carácter de Sujeto Obligado. Del mismo modo delimita las obligaciones de los responsables, encargados y usuarios de cada sistema y medidas de seguridad administrativa, física y técnica que deberán implementarse para el correcto manejo de la información que se posee. Lo anterior de conformidad a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, así como lo establecido en la Ley de Transparencia y Acceso a la Información del Estado de Jalisco y sus Municipios y su Reglamento.

El presente Documento de Seguridad fue elaborado por la Unidad de Transparencia y aprobado en su totalidad por el Comité de Transparencia, ambos de este Sujeto Obligado, mismo que será de observancia obligatoria para todos los trabajadores de este fideicomiso, así como para todas las personas externas que debido a la prestación de algún servicio deba tener acceso a la información, sistema o sitio web en el que se ubique cualquier tipo de dato personal protegido por este FIPRODEFO.

Sobre el Documento de Seguridad

El presente documento se refiere al instrumento que describe y da cuenta de manera general sobre las medidas de seguridad, técnicas, físicas y administrativas que ha adoptado el Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que se encuentran en posesión de este sujeto obligado.

De los Datos Personales

Los datos personales, así como la 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 información tal como nombre, domicilio, número de teléfono, número de seguridad social, datos relativos al patrimonio, las que se refieran a sus características físicas, morales o emocionales, a su vida familiar, entre otros.

Los Datos Personales Sensibles son aquellos que se refieren a la esfera íntima de su titular, o cuya utilización indebida puede dar origen a discriminación o conlleve un riesgo grave para éste. Tales como los relativos a su origen étnico o racial, estado de

salud, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencias sexuales u otros similares.[1]

Este FIPRODEFO deberá regirse y actuar bajo los principios enunciados en la Ley, como lo es la licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

Sobre el Aviso de Privacidad

Si los ciudadanos o instituciones privadas proporcionan al FIPRODEFO, información confidencial, este deberá de dar a conocer las políticas respecto de su protección, de conformidad con lo señalado por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado del Jalisco y sus Municipios y los Lineamientos que establezca el Instituto de Transparencia Acceso a la Información Pública y Protección de Datos Personales del Estado de Jalisco. El Aviso de Privacidad especifica las medidas que ha tomado el FIPRODEFO para garantizar la seguridad en el tratamiento de los datos personales que se recaban con motivo de trámites o del desempeño propio de las labores de este sujeto obligado, a través del cual se evita su alteración, pérdida, transmisión, publicación y acceso no autorizado.

Sobre los Derechos ARCO

Se trata de solicitudes sobre los datos personales que posee el sujeto obligado sobre los cuales se ejerce el derecho al Acceso, Rectificación, Cancelación y Oposición de los mismos, las cuales podrá realizar solamente el titular de los datos personales o su representante legal.

Es de vital importancia hacer hincapié que, para cualquier trámite relacionado al ejercicio de los Derechos ARCO, por razones de seguridad y protección de los datos personales que este sujeto obligado posee, debe ser demostrada la identificación plena del solicitante, a través de los medios legales establecidos para ellos (credencial INE, pasaporte vigente, cédula profesional, cartilla militar) tanto para solicitar la información como para recibirla.

La única instancia facultada dentro del FIPRODEFO para el tratamiento de los Datos Personales, es el Comité de Transparencia, mismo que entrará al estudio y evaluará la procedencia de las solicitudes de Derechos Arco de conformidad con la normativa estatal vigente, así como en base a los lineamientos dispuestos por el ITEI. El Comité de Transparencia deberá realizar una resolución debidamente fundada y motivada, la que será notificada al solicitante, respecto de la solicitud de cualquiera de los Derechos ARCO.

[1] Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, artículo 3 fracciones IX y X

El Tratamiento de la Información por parte de los Sujetos Obligados

Los sujetos obligados deberán adoptar las medidas necesarias para el debido tratamiento, manejo, mantenimiento, seguridad y protección de la información confidencial que obre en su poder, así como los procedimientos necesarios para garantizar la protección, tratamiento, mantenimiento, seguridad sobre el destino final de los datos personales que posean con motivo de sus atribuciones.

El tratamiento de datos personales, debe versar sobre toda aquella información que pueda encontrarse en cualquier material, ya sea en documento o medios digitales, como fotografías, grabaciones, soporte magnético, digital, sonoro, visual, electrónico, informático u otro elemento análogo.

De los Responsables y Encargados de la Protección de los Datos Personales e Información Confidencial

Solo podrán tener acceso a la información confidencial en posesión de este sujeto obligado, los miembros del Comité de Transparencia, el titular de la Unidad de Transparencia, los titulares de las Unidades Administrativas y/o los usuarios quienes por las labores que desempeñan, deberán de tener acceso a dicha información. Los anteriormente mencionados serán los responsables de resguardarla, así como promover las medidas necesarias para su tratamiento y custodia.

Por su parte el Comité de Transparencia, con ayuda de la Unidad de Transparencia, se encargará de establecer la información que tenga carácter de confidencial o reservada.

- Dictará las medidas necesarias para el tratamiento que deba darse a los datos personales en términos de las disposiciones legales aplicables, entendiendo en todo momento y como política institucional que estos tienen el carácter de reservada, salvo que se dicte disposición contraria por la autoridad competente para el caso concreto o que quien solicite la información sea el titular de la misma.

Medidas de Seguridad

Se trata de todas aquellas medidas que adopta el Comité de Transparencia y en su caso, en conjunto con el área que los posea, siempre que sea necesario para asegurar que la información confidencial y los datos personales sean resguardados de manera íntegra, segura y adecuada, ya sea a través de mecanismos administrativos, técnicos, físicos, políticas de procesos y controles.

De conformidad con lo señalado por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco, los deberes sobre la Seguridad de los datos personales, se entenderán tal y como lo marca el artículo 30 que a la letra dice:

*"**Artículo 30.** Deberes — Seguridad de los datos personales.*
1. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad; sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda, cuando éstas contemplen una protección mayor para el titular o complementen lo dispuesto en esta Ley y demás disposiciones aplicables."

Dentro de las medidas de seguridad que se tienen señaladas por la Ley y que deben ser seguidos los elementos que ahí se señalan, se encuentran:

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, formación 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 debe 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 fuera de las instalaciones de la organización; y*
d) *Proveer a los equipos que contienen o almacena datos personales de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad 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 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.*
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[2]

Con lo anterior se pretende que únicamente personal autorizado y plenamente identificado tenga acceso a los datos personales en posesión de este sujeto obligado y, así también, que el servidor público que tenga acceso a dicha información evite que ésta sea divulgada, a efecto de no comprometer la integridad, confiabilidad y disponibilidad de los sistemas de datos.

Objetivo de la Implementación de Medidas de Seguridad sobre los Datos Personales

Es atribución del Comité de Transparencia del FIPRODEFO establecer las recomendaciones sobre las políticas de manejo, mantenimiento, seguridad y protección de datos personales, que estén en posesión de las unidades administrativas de este fideicomiso, así como identificar aquellos datos que se recaban y poseen, las responsables, las encargadas y usuarios de cada sistema interno con los que se cuenta y las medidas de seguridad concretas implementadas por este sujeto obligado.

Por lo que es necesario promover la adopción de las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Para lograrlo se deben tomar en cuenta los avances tecnológicos, la naturaleza de los datos almacenados y los riesgos a que puedan estar expuestos, si provienen de la acción humana o de las condiciones físicas y ambientales, por lo que se han establecido distintos niveles de seguridad aplicables a cada categoría o tipo de datos alojados en los sistemas de datos personales.

Los alcances que deben de tener las recomendaciones son para convertirse en propuestas y sugerencias específicas para lograr la mayor protección de datos personales, por lo que las unidades administrativas del FIPRODEFO podrán utilizarlas como modelo a seguir y así tener la forma de seguridad sin perjuicio de que establezcan medidas adicionales que coadyuven a la mejor protección, la integridad, confidencialidad y disponibilidad de la información persona que se tiene.

El documento deberá mantenerse siempre actualizado y ser de observancia obligatoria para todos los trabajadores de este FIPRODEFO, así como para las personas externas que debido a la prestación de un servicio tengan acceso a determinado sistema o al sitio donde se ubican los mismos.

[2] Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, artículo 3, fracción XXV, XXVI, XXVII y XXVIII.

De los Niveles de Seguridad

En cuanto a los niveles de seguridad que se deben tomar respecto de la información que se posee, es necesario aclarar que los mismos no se encuentran establecidos en la legislación vigente, no obstante, es de gran importancia que este FIPRODEFO, establezca como políticas mínimas de actuación, aquellas contempladas en los estándares más altos y de mayor uso, y que sean tomadas como base para el tratamiento y resguardo de los datos personales con los que contamos.

En ese sentido, para este caso particular, tomaremos como referencia, el estándar internacional ISO/IEC 27002:2005, referente a las practicas sobre seguridad de información y que son tomadas a su vez como ejemplo por el Instituto Nacional de Transparencia en sus Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales.

Lo anterior a fin de garantizar la protección de datos personales que se tengan en posesión, estableciendo personal autorizado para la protección y promover el uso responsable de las nuevas tecnologías de la información, atendiendo los principios de protección de datos.

Por lo que tomando en cuenta los criterios establecidos sobre medidas de seguridad, para el resguardo eficaz de los datos personales, al final de cada medida, se establecen niveles de seguridad, las cuales deberán observarse atendiendo a la naturaleza de la información contenida en los sistemas establecidos.

Por lo tanto, las áreas que integran el FIPRODEFO aplicarán el nivel básico, medio o alto de medidas de seguridad, de acuerdo con la categoría o tipos de datos personales.

1. NIVEL BÁSICO. -

Estas medidas serán aplicables a todos los sistemas de datos personales[3]

- ***De Identificación:*** *Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma (en cuanto ésta no resulta confidencial cuando se emita en cumplimiento de la obligación legal para las funciones que fue contratado el servidor público y deba autorizar la emisión de un documento que por sus actividades resulta necesario para avalar el contenido del texto), firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.*

- ***Labores:*** *Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional (contraseña e información de procesos administrativos de la bandeja*

[3] Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales https://www.gob.mx/cms/uploads/attachment/file/83122/MODELOS_Y_GU_AS_17-pdf

de entrada), actividades extracurriculares, referencias laborales, referencias personales entre otros.

La posesión de datos personales deberá obedecer exclusivamente a las atribuciones legales o reglamentarias de cada entidad y deberán obtenerse a través de los medios previstos; estos datos sólo deberán tratarse únicamente para la finalidad para la cual fueron obtenidos.

Cuando los datos personales se actualicen no deben de alterar la veracidad de la información que tengan y debe de ser por personal autorizado para el cumplimiento de las atribuciones de este FIPRODEFO.

2. NIVEL MEDIO. -

Los datos personales además de cumplir con las medidas de seguridad de nivel básico, deberán observar las marcadas en el nivel medio[4]

- ***Datos Patrimoniales:*** *Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.*

- ***Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales:*** *Información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.*

- ***Datos Académicos:*** *Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.*

- ***Tránsito y movimientos migratorios:*** *Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas entre otros.*

Este tipo de datos debido a la trascendencia para la intimidad, se debe evitar prejuicios por el uso que se pueda hacer con ese tipo de información siendo factores de generar graves conflictos, si no tienen el debido cuidado al manejar la información confidencial.

3. NIVEL ALTO. -

Los datos personales que contengan algún dato que se enliste deberán cumplir con las medidas de seguridad de nivel básico y medio, deberán observar las marcadas con el nivel alto.

[4] IBID página 14

- ***Datos Ideológicos:*** *Creencia religiosa, ideología, filosófica, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.*

- ***Datos de Salud:*** *Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.*

- ***La ubicación de menores de edad:*** *a través de sus datos académicos y toda la información que se posea de estos, toda vez que la revelación de algún dato personal puede poner en riesgo la integridad de menores.*

- ***Características personales:*** *Tipo de sangre, ADN, huella digital, u otros análogos.*

- ***Características físicas:*** *Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otras.*

- ***Vida sexual:*** *Preferencia sexual, hábitos sexuales, entre otros.*

- ***Origen:*** *Étnico y racial.*

Los niveles de protección señalados definen el mayor o menor grado de confidencialidad, disponibilidad e integridad que el sujeto obligado debe asegurar de acuerdo con la naturaleza de los datos personales que custodia, de conformidad con las siguientes definiciones:

*La **confidencialidad** es asegurar que la información no sea accedida por – o divulgada a- personas o procesos no autorizados.*

*La **integridad** es garantizar la exactitud y la confiabilidad de la información y los sistemas de manera que éstos no puedan ser modificados sin autorización, ya sea accidental o intencionalmente.*

*La **disponibilidad** es que las personas o procesos autorizados accedan a los activos de información cuando así lo requieran*[5]

[5] Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales. http://www.gob.mx/cms/uploads/attachment/file/83122/MODELOS_Y_GU_AS_17.pdf

Accesos Controlados y Bitácoras

Deberá guardarse como mínimo los datos completos del responsable, encargado o usuario, el modo de autenticación del responsable, encargado o usuario, fecha y hora en se realizó el acceso, o se intentó el mismo sistema de datos personales accedido, operaciones o acciones llevadas a cabo dentro del sistema de datos personales, fecha y hora en que se realizó la salida del sistema de datos personales.[6]

Operaciones de Acceso, Actualización, Respaldo y Recuperación.

Se debe de contar con manuales de procedimientos y funciones para el tratamiento de datos personales que deberán observar obligatoriamente los responsables, encargados o usuarios de los sistemas de datos personales.[7]

Llevar control y registros del sistema de datos personales en bitácoras que contengan la operación cotidiana, respaldos, usuarios, incidentes y accesos, así como la transmisión de datos y sus destinatarios, de acuerdo con las políticas internas que establezca la entidad.

Procedimientos de control de acceso a la red que incluyan perfiles de usuarios o grupos de usuarios para el acceso restringido a las funciones y programas de los sistemas de los datos personales.

Deberán contar con mecanismos de auditoría o rastreabilidad de operaciones y así garantizar que el personal encargado del tratamiento de datos personales sólo tenga acceso a las funciones autorizadas del sistema de datos personales según su perfil de usuario. Aplicar procedimientos de respaldo de base de datos y realizar pruebas periódicas de restauración, se tendrá que llevar el control de inventarios y clasificación de los medios magnéticos u ópticos de respaldo de los datos personales.

Utilizar un espacio externo seguro para guardar de manera sistemática los respaldos de base de datos personales y el transporte de los sistemas de datos personales, se debe garantizar que, durante la transmisión de datos personales y el transporte de los soportes de almacenamiento, que no se pueda tener acceso a los datos, que no sean, reproducidos, alterados o suprimidos sin autorización.

La aplicación de los procedimientos para la destrucción de medios de almacenamiento y de respaldo obsoletos que contengan datos personales. En los casos en que la operación sea externa, convenir con el responsable de cada unidad administrativa

[6] GUIA PARA LA ELABORACIÓN DE UN DOCUMENTO DE SEGURIDAD V 1.4

[7] IBID

que tenga la facultad de verificar que se respete la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales, revisar que el tratamiento se está realizando conforme a lo establecido.

Diseñar planes de contingencia que garanticen la continuidad de la operación y realizar pruebas de eficiencia de los mismos.

Llevar a cabo las verificaciones a través de las áreas de tecnología de la información, informática o su equivalente y cualquier otra medida tendente a garantizar el cumplimiento de los principios de protección de datos personales.[8]

[8] IBID

SISTEMAS DE SEGURIDAD, IDENTIFICACIÓN Y NIVELES DE SEGURIDAD POR UNIDAD ADMINISTRATIVA A TRAVÉS DEL ORGANIGRAMA DEL FIPRODEFO.

DIRECCIÓN GENERAL

DATOS DE IDENTIFICACIÓN			
Fecha de Elaboración	Día 16	Mes 08	Año 2019
Sujeto Obligado	Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco		
Unidad Administrativa Responsable	Dirección General		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	1. Correos electrónicos 2. Números de Teléfono		
Personas o grupos de personas sobre las cuales se obtienen los datos	Físicas / Morales		
Procedimiento de recolección	Físico / Electrónico		
Tipo de soporte en donde se contienen los datos personales	Físico / digital		
Características del lugar de resguardo	La información recolectada se resguarda en archiveros, cajas o muebles de las oficinas del área generadora de la información.		
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Dirección General	Mtro. Arturo Pizano Portillo	Director General	

ADMINISTRADORES		
Área	Administrador	Cargo
Dirección General	Imelda Rivera Escobedo	Asistente de Dirección
DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO		
TIPO DE DATOS PERSONALES		
Nombre, Domicilio, correos electrónicos, teléfono, firmas		
Tipo de Tratamiento	Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.	
TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL		
1. Correos electrónicos 2. Números de Teléfono		La información es susceptible a transferirse a todas las coordinaciones que integran este Fideicomiso
Nivel de protección exigible.	x	Básico
		Medio
		Alto
FUNDAMENTACIÓN		
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.		

COORDINACIÓN ADMINISTRATIVA

DATOS DE IDENTIFICACIÓN			
	Día	Mes	Año
Fecha de Elaboración	16	08	2019
Sujeto Obligado	Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco		
Unidad Administrativa Responsable	Coordinación Administrativa		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	1. Pago a proveedores. 2. Expedientes de recursos humanos del personal de estructura y el personal subcontratado. 3. Pago de nóminas. 4. Pago de beneficiados por Reglas de Operación. 5. Expedientes de licitaciones con Concurrencia de Comité y sin Concurrencia de Comité.		
Personas o grupos de personas sobre las cuales se obtienen los datos	1. Físicas y morales que son proveedores de servicios o bien 2. Personal de Estructura de FIPRODEFO y personal sub contratado.		
Procedimiento de recolección	Físico/ digital		
Tipo de soporte en donde se contienen los datos personales	Físico/ digital		
Características del lugar de resguardo	La información recolectada se resguarda en archiveros, cajas o muebles y plataformas de las oficinas del área generadora de la información.		
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Coordinación Administrativa	Lic. Margarita Elizabeth Cordova	Coordinadora Administrativa	

	Torres	

ADMINISTRADORES		
Área	Administrador	Cargo
Coordinación Administrativa	Luz María Muñoz López	Analista Especializado
Coordinación Administrativa	Carlos Rodrigo Méndez Narvaez	Auxiliar Administrativo
Coordinación Administrativa	Miguel Ángel Bonilla Cancino	Asesor Contable

DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO	
TIPO DE DATOS PERSONALES	
1. RFC de personas Morales y Físicas. 2. CURP 3. Comprobantes de domicilios. 4. Actas Constitutivas 5. Estados de Cuenta bancarios. 6. Curriculum. 7. Correos electrónicos personales. 8. Números de celular.	
Tipo de Tratamiento	Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.
TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL	
Los expedientes del personal sub contratado se transfieren a la empresa adjudica en la licitación.	

Nivel de protección exigible.		
		Básico
	X	Medio
		Alto

FUNDAMENTACIÓN
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

COORDINACIÓN DE GEOMÁTICA

DATOS DE IDENTIFICACIÓN			
	Día	Mes	Año
Fecha de Elaboración	16	08	2019
Sujeto Obligado	Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco		
Unidad Administrativa Responsable	Coordinación de Geomática		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	1.- Capacitaciones técnicas al personal institucional y a la ciudadanía en general interesada. 2- Expedientes de atención a solicitudes de información geográfica y acciones de seguimiento de respuesta.		
Personas o grupos de personas sobre las cuales se obtienen los datos	1- Ciudadanos que emiten oficios de solicitud de información geográfica 2- Personas o instituciones que solicitan cursos de formación técnica geográfica. 3- Personal universitario, técnicos forestales, institucionales y ciudadanía en general que acuden a los cursos de capacitación.		
Procedimiento de recolección	1- Telefónica, oficiosa, por correo electrónico, derivadas de otras instituciones o cabeza de sector. 2- Listas de asistencia, encuestas de evaluación.		
Tipo de soporte en donde se contienen los datos personales	Físico / Digital		
Características del lugar de resguardo	La información recolectada se resguarda en archiveros, cajas o muebles y plataformas de las oficinas del área generadora de la información.		
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Coordinación de Geomática	Lic. Hugo Enrique Nolasco Reyes	Coordinador de Geomática	

ADMINISTRADORES		
Área	Administrador	Cargo
Coordinador de Geomática	José Isaac Márquez Rubio	Técnico en Geomática
DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO		
TIPO DE DATOS PERSONALES		
Nombre, Cargo o puesto, correo electrónico particular, número celular particular.		
Tipo de Tratamiento	Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.	
TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL		
No aplica		
Nivel de protección exigible.	X	Básico
		Medio
		Alto
FUNDAMENTACIÓN		
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.		

COORDINACIÓN DE BOSQUES

DATOS DE IDENTIFICACIÓN			
	Día	Mes	Año
Fecha de Elaboración	16	08	2019
Sujeto Obligado	Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco		
Unidad Administrativa Responsable	Coordinación de Bosques		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	1.-Conformación de Expedientes de solicitudes para acceso de apoyos económicos 2.- Capacitaciones a personal técnico		
Personas o grupos de personas sobre las cuales se obtienen los datos	1.-Ciudadanos que emiten solicitudes para acceso de apoyos económicos para sus predios, ejidos o comunidades indígenas 2.- Personal de dependencias estatales, federales, municipales, asociaciones y ciudadanía en general, que acude a los cursos de capacitación.		
Procedimiento de recolección	1.-Recepción física de documentos en sedes previamente designadas 2.- A través de correo electrónico oficial		
Tipo de soporte en donde se contienen los datos personales	1.-Expedientes de los documentos en físico con claves previamente designadas y almacenados en cajas exprofeso. 2.- Forma digital con respaldos de seguridad		
Características del lugar de resguardo	La información recolectada se resguarda en archiveros, cajas o muebles de las oficinas del área generadora de la información.		
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Coordinación de Bosques	Ing. Alfredo Martínez Moreno	Coordinador de Bosques	

ADMINISTRADORES		
Área	Administrador	Cargo
Coordinación Bosques	Biol. Patricia Rojas Sánchez	Auxiliar Coordinación de Bosques

DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO	
TIPO DE DATOS PERSONALES	
Tipo de Tratamiento	Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.

TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL		
Nivel de protección exigible.		Básico
	X	Medio
		Alto

FUNDAMENTACIÓN
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

COORDINACIÓN DE SANIDAD

DATOS DE IDENTIFICACIÓN			
Fecha de Elaboración	Día 16	Mes 08	Año 2019
Sujeto Obligado	Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco		
Unidad Administrativa Responsable	Coordinación de Sanidad		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	1.-Seguimiento de instalación de viveros rústicos y producción de planta. 2.- Cursos de capacitación.		
Personas o grupos de personas sobre las cuales se obtienen los datos	1.- Beneficiarios de las ROP 2.- Ciudadanía que requiera la información (productores)		
Procedimiento de recolección	1.-Formato 2.- Lista de asistencia		
Tipo de soporte en donde se contienen los datos personales	Físico/Digital		
Características del lugar de resguardo	La información recolectada se resguarda en archiveros, cajas o muebles y plataformas de las oficinas del área generadora de la información.		
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Coordinación de Sanidad	Mtra. Gloria Iñiguez Herrera	Coordinadora de Sanidad	

ADMINISTRADORES		
Área	Administrador	Cargo
Coordinación de Sanidad	Álvaro Xicohtencatl Hernández	Apoyo Técnico Sanidad

DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO	
TIPO DE DATOS PERSONALES	
Nombre, correo electrónico, teléfono	
Tipo de Tratamiento	Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.

TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL		
Nivel de protección exigible.	x	Básico
		Medio
		Alto

FUNDAMENTACIÓN
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

COORDINACIÓN DE GENÉTICA FORESTAL

DATOS DE IDENTIFICACIÓN			
Fecha de Elaboración	Día 16	Mes 08	Año 2019
Sujeto Obligado	Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco		
Unidad Administrativa Responsable	Coordinación de Genética Forestal		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	1.- Seguimiento ROP		
Personas o grupos de personas sobre las cuales se obtienen los datos	1.- Beneficiarios de las ROP		
Procedimiento de recolección	1.- Física/Digital		
Tipo de soporte en donde se contienen los datos personales	1.- Física/Digital		
Características del lugar de resguardo	La información recolectada se resguarda en archiveros, cajas o muebles y plataformas de las oficinas del área generadora de la información.		
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Coordinación de Genética Forestal	Ing. Antonio Vieyra Ramírez	Coordinador de Genética Forestal	

ADMINISTRADORES		
Área	Administrador	Cargo

DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO		
TIPO DE DATOS PERSONALES		
Nombre, correo electrónico, teléfono		
Tipo de Tratamiento	Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.	
TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL		
No aplica		
Nivel de protección exigible.	X	Básico
		Medio
		Alto
FUNDAMENTACIÓN		
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.		

Área Legal

DATOS DE IDENTIFICACIÓN			
	Día	Mes	Año
Fecha de Elaboración	16	08	2019
Sujeto Obligado	Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco		
Unidad Administrativa Responsable	Área legal		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	Para acreditar su representatividad en la firma del documento legal		
Personas o grupos de personas sobre las cuales se obtienen los datos	Personas físicas y morales; entidades y dependencias gubernamentales.		
Procedimiento de recolección	A través de instrumentos legales		
Tipo de soporte en donde se contienen los datos personales	Físico/digital		
Características del lugar de resguardo	La información recolectada se resguarda en archiveros, cajas o muebles de las oficinas del área generadora de la información.		
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Dirección General	Mtro. Arturo Pizano Portillo	Director General	

ADMINISTRADORES		
Área	Administrador	Cargo
legal	Gracia Elizabeth Carlo Pérez	Asesor legal

DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO		
TIPO DE DATOS PERSONALES		
Nombre, domicilio, RFC, CURP, fotografía, cuentas bancarias, estado civil, etnia, nacionalidad.		
Tipo de Tratamiento	Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.	
TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL		
No aplica		
Nivel de protección exigible.		Básico
	X	Medio
		Alto
FUNDAMENTACIÓN		
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios. Acreditación de personalidad: Nombre, CURP, fotografía, estado civil, nacionalidad; Su requerimiento se fundamenta en los Artículos 1, 2 y 90 del Código de Procedimientos Civiles del Estado de Jalisco. Domicilio; Su requerimiento se fundamenta en los Artículos 107 y 161 del Código de Procedimientos Civiles del Estado de Jalisco. Etnia Su requerimiento se fundamenta en el Artículo 87 del Código de Procedimientos Civiles del Estado de Jalisco asi como en Ley Sobre Los Derechos Y El Desarrollo De Los Pueblos Y Las Comunidades Indígenas Del Estado De Jalisco en su artículo 4.		

UNIDAD DE TRANSPARENCIA

DATOS DE IDENTIFICACIÓN			
	Día	Mes	Año
Fecha de Elaboración	16	08	2019
Sujeto Obligado	Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco		
Unidad Administrativa Responsable	Unidad de Transparencia		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	1.-Conformación de Expedientes de solicitudes de acceso a la información. 2.- Capacitaciones al personal y a la ciudadanía en general		
Personas o grupos de personas sobre las cuales se obtienen los datos	1.-Ciudadanos que emiten solicitudes de acceso a la información. 2.- Personal del FIPRODEFO y ciudadanía en general que acude a los cursos de capacitación.		
Procedimiento de recolección	1.-Solicitudes recibidas por Plataforma Nacional de Transparencia, Oficialía de partes, correo electrónico, vía telefónica y remitidas por otras dependencias o entidades. 2.- Listas de Asistencia		
Tipo de soporte en donde se contienen los datos personales	Físico/Digital		
Características del lugar de resguardo	La información recolectada se resguarda en archiveros, cajas o muebles de las oficinas del área generadora de la información.		
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Unidad de Transparencia	Lic. Hugo Enrique Nolasco Reyes	Titular de la Unidad de Transparencia	

ADMINISTRADORES		
Área	Administrador	Cargo
Unidad de Transparencia	Lic. Laura Nayeli Pacheco Casillas	Analista de Transparencia

DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO	
TIPO DE DATOS PERSONALES	
Nombre, Teléfono particular, Domicilio, Correo electrónico	
Tipo de Tratamiento	Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.

TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL		
Unidades internas, sujetos obligados y/o autoridades que en su caso sea requerido ceder los datos		Finalidad
Nivel de protección exigible.		Básico
	X	Medio
		Alto

FUNDAMENTACIÓN
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

De las Funciones y Obligaciones de los Servidores Públicos que tratan los Datos Personales.

Para garantizar la aplicación correcta de este sistema es necesario establecer los deberes de los servidores públicos del FIPRODEFO que participan en el tratamiento de los datos personales derivado de sus atribuciones.

Al momento de recibir los datos personales el servidor público que se encargue de su recepción deberá:

1) Tener a la vista el Aviso de Privacidad.
2) Dar a conocer el Aviso de Privacidad al titular de los datos personales previo a la obtención de sus datos.
3) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia.
4) Al obtener los datos personales cerciorarse de que la información esté completa, actualizada, sea veraz, y comprensible.
5) Comunicar discrepancias de los datos personales recabados a su jefe inmediato o al administrador de los datos personales, ello cuando se dé cuenta.
6) Conocer y seguir las medidas de seguridad que le sean aplicables para el cuidado de los datos personales, durante el periodo en el que posea los datos personales.
7) Recabar los datos personales para la finalidad para la cual estos fueron recabados según el sistema de tratamiento que corresponda.
8) Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.
9) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del FIPRODEFO, en el tratamiento de datos personales.
10) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
11) Tomar, una vez al año un curso, taller o capacitación sobre el tratamiento de datos personales.
12) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.
13) Abstenerse de realizar transferencias de datos personales que no vayan de conformidad con la finalidad para la cual se obtuvieron los datos.

El servidor público que administra los datos personales, conforme los sistemas de tratamiento vigentes deberán:

1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del FIPRODEFO, en el tratamiento de datos personales.
2) Conocer e implementar las medidas de seguridad establecidas en el Documento de Seguridad.
3) Aplicar nuevas medidas de seguridad que resulten accesibles y viables para la protección de datos personales.

4) Supervisar a los servidores públicos que participan en la recepción y en el tratamiento de datos personales en cada sistema.
5) Tratar los datos personales para la finalidad para la cual estos fueron recabados según el sistema de tratamiento que corresponda.
6) Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.
7) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
8) Tomar, una vez al año, un curso, taller o capacitación sobre el tratamiento de datos personales.
9) Informar a los titulares de los datos sobre nuevas finalidades del tratamiento de datos personales o nuevas transferencias.
10) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia.
11) Informar a la Unidad de Transparencia sobre los cambios que sufran sus sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.
12) Acudir a la Unidad de Transparencia en caso de asesoría sobre el tratamiento de datos personales.
13) Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de las mismas.
14) Dar aviso al Comité de Transparencia, a través del la Unidad de Transparencia, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.
15) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

El servidor público responsable de cada sistema, o en su caso, el titular de la Unidad Administrativa responsable de cada sistema deberá:

1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del FIPRODEFO, en el tratamiento de datos personales.
2) Implementar las medidas de seguridad que establece el Documento de Seguridad.
3) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
4) Tomar una vez al año un curso, taller o capacitación sobre el tratamiento de datos personales.
5) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia.
6) Aplicar medidas correctivas en caso de identificar incidentes, alteraciones o vulneraciones en el tratamiento de datos personales.

7) Informar a la Unidad de Transparencia sobre los cambios que sufran sus sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.
8) Monitorear la implementación de las medidas de seguridad.
9) Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de las mismas.
10) Dar aviso al Comité de Transparencia, a través del la Unidad de Transparencia, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.
11) Presentar propuestas de mejora o modificación del documento de seguridad a través de la Unidad de Transparencia.
12) Emitir reportes en relación al tratamiento de los datos personales y la aplicación de medidas de seguridad, según sea requerido por el Comité de Transparencia a través de la Unidad de Transparencia.
13) Diseñar, desarrollar e implementar políticas públicas, procesos internos, y/o sistemas o plataformas tecnológicas necesarias para el ejercicio de sus funciones apegándose en todo momento al Documento de Seguridad, las políticas o lineamientos que para el tratamiento de datos personales emita el Comité de Transparencia, la Unidad de Transparencia y el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI), así como a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.
14) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

Son obligaciones de la Unidad de Transparencia en relación al tratamiento de datos personales, además de las previstas en el artículo 88 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco:

1) Difundir al interior del FIPRODEFO el Aviso de Privacidad y el Documento de Seguridad.
2) Revisión física anual sobre el tratamiento de datos personales y la implementación de medidas de seguridad.
3) Proponer al Comité de Transparencia actualizaciones o modificaciones al documento de seguridad.
4) Emitir un reporte anual al Comité de Transparencia sobre el ejercicio de estas funciones.

Son obligaciones del Comité de Transparencia en relación al tratamiento de datos personales, además de las previstas en el artículo 87 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco:

1) Revisar anualmente las políticas y/o lineamientos en materia de protección de datos personales establecidos en el presente documento. 2) Emitir o aprobar anualmente un programa de capacitaciones en materia de protección de datos personales.

3) Requerir anualmente a las unidades administrativas que tratan datos personales, a través de la Unidad de Transparencia, informes sobre el tratamiento de los datos personales y la aplicación de medidas de seguridad, así como vulneraciones detectadas en el año.

ANÁLISIS DE RIESGOS

Debido a las circunstancias generales, tanto físicas como humanas, en las que se tratan datos personales, se ha logrado identificar los siguientes riesgos posibles ante los que se pudiera enfrentar este Sujeto Obligado:

- Insuficiencia presupuestal para cumplir con las disposiciones del Ley.
- Obtención de datos incompletos o incorrectos.
- Omitir la notificación al titular de los datos personales del Aviso de Privacidad.
- No difundir el Aviso de Privacidad.
- Ante la necesidad de tener un consentimiento expreso: no tener evidencia de que el titular de los datos personales conoce los términos del Aviso de Privacidad.
- No tener un lugar seguro y de acceso restringido en donde se puedan archivar los datos personales en físico.
- Permitir a todo servidor público o personas ajenas a la dependencia, el acceso a los expedientes que contienen datos personales.
- Pérdida de expedientes físicos debido a catástrofes, inundaciones, e incendios.
- Daño de la base de datos que contenga información confidencial.
- Fallas en los equipos de cómputo en donde se encuentran las bases de datos.
- Falta de capacitación de los servidores públicos en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan debido al desempeño de sus funciones.
- Pérdida, robo o extravío de expedientes.
- Alteración de la información.

Ante dichos riesgos identificados es necesario hacer un análisis de estos, amenazas y sus posibles vulneraciones.

Origen de la Amenaza	Causa	Posibles Consecuencias
Acceso de personas no autorizadas a los sistemas o plataformas oficiales del FIPRODEFO	Adquirir información o datos personales.	Acceso no autorizado. Divulgación de datos personales. Robo de información. Modificaciones no autorizadas.
Personal del sujeto obligado con poco conocimiento sobre el tratamiento de datos personales.	Obtener información para beneficio personal. Curiosidad. Error involuntario. Por fines económicos.	Ataque a otros servidores públicos. Robo de información. Pérdida de datos personales. Uso indebido de datos personales. Uso ilícito de datos personales. Extorsión. Modificaciones no autorizadas.
Daño físico	Corrosión. Agua. Fuego. Accidentes.	Daño o pérdida de los datos personales.
Eventos naturales.	Desastres climatológicos. Fenómenos meteorológicos. Sismos. Cualquier eventualidad por causa natural.	Daño o pérdida de los datos personales.
Fallas técnicas.	Pérdida de electricidad. Falla o pérdida de internet. Falla en sistemas, correos electrónicos o plataformas oficiales.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas.

Decadencias técnicas.	Mantenimiento insuficiente. Falla en equipos. Poca o absoluta renovación de equipos de telecomunicaciones o cómputos. Cambios de voltaje.	Pérdida, destrucción y daño.
Susceptibilidad en redes o sistemas autorizados.	Falta de contraseñas altamente efectivas. Falta de mecanismos para identificar o autenticación de usuarios. Falta de actualización de antivirus.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Organización.	Procesos carentes de formalidad para administración, acceso, uso y proceso de archivo.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Espacio donde se archiven.	Carencia de un servidor o sistema que almacene los datos personales. La falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado al área donde se almacenan o archivan los datos personales (en su caso los expedientes que los contengan), es un escenario de vulneración y riesgo, facilitando el mal manejo de los datos personales y la pérdida, robo o extravío de expedientes.	Daño y/o pérdida de los datos personales. Modificaciones no autorizadas.

Hasta el momento no se han identificado o reportado vulneraciones desde las unidades administrativas generadoras de información que integran el Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco.

ANÁLISIS DE BRECHA

Una vez identificados los posibles riesgos a los que este Sujeto Obligado se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base las entrevistas que se hicieron con las diferentes Unidades Administrativas de este FIPRODEFO.

Las unidades administrativas reportaron las siguientes medidas de seguridad existentes:

- Quien recaba los datos personales, es un trabajador del área, asignado especialmente para recabar datos en general necesarios para cada sistema
- El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones o fuera de ellas según las necesidades del área generadora de la información.
- Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.
- En la mayoría de las áreas, el acceso (al área donde se recibe a los ciudadanos y se recaban datos personales) se tiene restringido, una vez que el dato se encuentra en posesión del empleado, es decir si fue recabado frente a un escritorio, ventanilla, área abierta o pasillo, los ciudadanos no podrán pasar detrás de estos, ya que al terminar de recabar datos estos se colocan fuera del alcance de los ciudadanos.
- Las llaves que se tienen de cada área se encuentran en manos de servidores públicos, autorizados.
- Una vez recabados los datos personales, el empleado genera un expediente, del cual se obtuvieron los datos personales, ya sea físico o electrónico.
- Una vez recabados los datos personales, ya realizada la carpeta o expediente (electrónica, física, en plataformas, o cualquiera generada) y guardada esta en archiveros o puesta en resguardo electrónico, tienen acceso a esta área empleados autorizados.
- Las llaves de los archiveros con las que se cuentan se encuentran en posesión de empleados encargados del área.
- Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el empleado guarda los mismos en carpeta electrónica, ya sea en su computadora, carpeta compartida, correo electrónico oficial o plataforma.
- Durante el desahogo, procedimiento por el cual se obtuvieron los datos personales, los empleados del área tienen acceso a los datos personales.
- Los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del procedimiento al que pertenecen y resguardados por el área responsable de la información.

Las medidas de seguridad que actualmente se llevan a cabo pudieran ser efectivas de aplicarse de manera continua y consciente en las áreas administrativas del sujeto obligado. El riesgo latente que se provoca por la falta de conocimiento, o compromiso para la aplicación de estas medidas existentes se puede minimizar por medio del establecimiento obligatorio de dichas medidas de seguridad y de la mejora continua de las mismas.

DE LAS MEDIDAS DE SEGURIDAD

Con base en lo anterior se establecen las siguientes medidas de seguridad de carácter físico, técnico y administrativo:

Objetivo del Control	Descripción
Control de empleados que recaban los datos personales.	Debe realizarse un listado de los empleados que recaban datos personales, esto es, del personal que tiene contacto con el titular de los datos personales por sus funciones.
Control de empleados que recaban los datos personales.	Forzosa asistencia a por lo menos a 1 capacitación en materia de datos personales impartida por la Unidad de Transparencia.
Control de empleados que recaban los datos personales.	Remitir el Documento de Seguridad para el conocimiento y cumplimiento de las medidas de seguridad aplicables para un correcto tratamiento de datos personales.
Aviso de privacidad.	El empleado que reciba los datos personales, deberá tener a la vista de todos los ciudadanos el aviso de privacidad, y darlo a conocer al momento de recabar los datos.
Aviso de privacidad.	Si se cuenta con un formato, este deberá contener la mención y debe dar a conocer el Aviso de Privacidad del FIPRODEO, ya sea simplificado o la liga de internet que remita al ciudadano al Aviso de Privacidad. Los formatos nuevos que se impriman posteriores a la emisión del presente documento deberán contar con la liga al Aviso de Privacidad
Aviso de privacidad.	Si el dato personal fue recabado mediante una plataforma electrónica oficial, esta plataforma deberá contener la mención y debe dar a conocer el Aviso de Privacidad del FIPRODEFO, ya sea simplificado o la liga de internet que remita al ciudadano al Aviso de Privacidad.
Espacio físico.	El área específica que recabe los datos deberá contar con puertas que tengan llave, sin excepción alguna, para asegurar de forma efectiva el trato adecuado de los datos personales, así evitar mal uso de los mismos o vulneraciones.
Espacio físico.	Las llaves de las puertas de cada unidad administrativa, deberán ser guardadas únicamente por servidores públicos empleados del área, autorizados para poseer las llaves.
Espacio físico.	Al término de las labores, deberá cerrarse cada oficina de las áreas, para evitar el contacto de otros empleados o ciudadanos con los datos personales recabados.
Espacio físico.	Al concluir la jornada laboral, se deberá guardar los expedientes, para no dejarlos al alcance de ciudadanos o personal no autorizado.
Archivo	Al finalizar el desahogo de los expedientes estos deberán archivarse en un lugar adecuado con las siguientes características: · No estar al alcance de los ciudadanos o empleados ajenos al área. · Deberá ser un área específica para guardar los expedientes. · Este archivo debe estar bajo llave. · La llave del mismo solo puede estar en manos de personal autorizado para esto.

Acceso al Archivo	Se deberá crear por cada área, un control o bitácora del personal que tiene acceso al archivo, el control debe contener lo siguiente: · Registro para anotar el nombre y puesto del personal autorizado. · Fecha, hora de entrada y hora de salida del archivo. · Registrar el expediente que se consultó. · Registrar el expediente que se extrae del archivo, y fecha en la que se regresa el expediente. · Firma de conformidad del personal que entró. · Firma de consentimiento del personal autorizado para llevar el control de este archivo.
Control de Archivos Electrónicos	Cuando los datos personales sean recabados por medios electrónicos, se deberá generar expediente, dicho expediente deberá ser guardado en base de datos, correo electrónico oficial, o en plataforma autorizada, no en cualquier plataforma o correo electrónico personal.
Control de Archivos Electrónicos	Para evitar riesgos, respecto a los expedientes electrónicos, se debe contar con un respaldo electrónico. Dicho respaldo deberá realizarse, como mínimo, de manera anual.
Transferencia de datos personales.	En caso de ser necesario derivado de las funciones del área, por requisito del trámite, se deba realizar una transferencia de datos personales, se deberá informar al sujeto que reciba los datos el Aviso de Privacidad para que se sujete al mismo.
Versiones Públicas	En los casos en los cuales se realicen clasificaciones de información confidencial, que incluyan datos personales, los documentos que contengan los datos, deberán entregarse siempre en versión pública, adjuntando índice de datos personales.

Medidas de seguridad para transferencias:

Transferencias al interior del sujeto obligado y a otros sujetos obligados:

- Solo podrán ser transferidos los datos personales para dar seguimiento y conclusión al trámite o sistema de tratamiento bajo la finalidad que éstos prevean.
- El área que entrega los datos personales deberá cerciorarse de transferir la totalidad de los datos que resulten necesarios para el seguimiento o la conclusión del trámite o sistema de tratamiento correspondiente. Limitándose a la entrega de datos adicionales que no resulten necesarios.
- El área que entrega los datos personales deberá cerciorarse de que los datos que transfiere sean completos y veraces.
-El área que reciba los datos personales deberá conservar los mismos sujetándose a las finalidades y lineamientos del Aviso de Privacidad de este sujeto obligado y adoptando las medidas de seguridad previstas en este documento.
- El área que reciba los datos personales deberá encargarse de la supresión de los datos que reciba cuando esta corresponda.

- El área que entrega y el área que recibe los datos personales deberán dar acceso a los datos personales, tratándose de procedimientos de derecho ARCO.

Transferencias a terceros:

- El tercero que reciba los datos personales deberá sujetarse a las finalidades y lineamientos del Aviso de Privacidad de este sujeto obligado y deberá adoptar las medidas de seguridad previstas en este documento.
- En caso de ser necesario conforme a las disposiciones normativas, se deberá firmar un convenio o acuerdo de confidencialidad que proteja el tratamiento de los datos personales que recaba este sujeto obligado y transfiere al tercero

Medidas de seguridad en caso de vulneraciones a la seguridad:

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias, misma que deberá seguirse bajo el siguiente formato y ejemplo:

Fecha en la que ocurrió	Motivo	Las acciones correctivas implementadas de forma inmediata y definitiva
05/03/2020	Incendio	Impresión del expediente. Generar nuevo expediente electrónico.

Después del registro, se deberá informar de forma inmediata al titular y al Instituto las vulneraciones de seguridad ocurridas, las que afecten o impacten de forma significativa los derechos patrimoniales o morales del titular, en un plazo máximo de setenta y dos horas en cuanto se confirmen y este en proceso las acciones encaminadas para dimensionar la afectación, con la finalidad de que los titulares puedan tomar medidas correspondientes para la defensa de sus derechos, dicha notificación debe contener lo siguiente:

I. La naturaleza del incidente.
II. Los datos personales comprometidos.
III. Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses.
IV. Las acciones correctivas realizadas de forma inmediata.
V. Los medios donde puede obtener mayor información al respecto.

Al ocurrir una vulneración de seguridad, el encargado del área responsable y/o el responsable del sistema deberá analizar la causa por lo que ocurrió dicha vulneración, e implementar y anexar a su plan de trabajo las acciones preventivas y correctivas para adecuar medidas de seguridad que prevengan esta eventualidad, para evitar que la vulneración se repita. A su vez, en caso de detectar que la falla fue ocasionada por el

incumplimiento de un empleado a su cargo, deberá levantar acta circunstanciada de hechos correspondiente y seguir el
procedimiento administrativo correspondiente ante el Titular fideicomiso.

Medidas de seguridad o controles para la identificación y autentificación de usuarios:

Parte de tener control efectivo al trato de los datos personales es contar con un sistema que garantice la autenticación de usuarios, esto es por medio de administración de cuentas creadas específicamente para cada servidor público. La administración de cuentas de usuario es una parte esencial de los sistemas que se desarrollan en el departamento de software. La razón principal de las cuentas de usuario es verificar la identidad de cada funcionario también permite la utilización personalizada de acceso a la información y generación de la misma. Esta medida es tomada para los correos electrónicos institucionales y para cualquier sistema o plataforma tecnológica que cree este sujeto obligado. El estándar para la creación de las cuentas es:

Usuario: Generalmente es el correo electrónico institucional

Contraseña: Frase de confirmación de identidad que se encuentra encriptada para mayor seguridad

Medidas de Seguridad para la Supresión y Borrado Seguro de Datos Personales

Todos los datos personales en posesión del sujeto obligado sin importar el soporte en el que se encuentren deberán ser tratados para la supresión y borrado conforme a las técnicas de supresión y borrado seguro de datos personales.

Las técnicas de supresión y borrado seguro de datos personales son las siguientes:

Métodos Físicos

1. Trituración mediante corte cruzado o en partículas: Cortar el documento de forma vertical y horizontal generando fragmentos diminutos, denominados "partículas", lo cual hace prácticamente imposible que se puedan unir.

2. Destrucción de los medios de almacenamiento electrónicos mediante desintegración, consistente en separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.

Métodos Lógicos

Sobre-escritura: consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

De conformidad con el artículo 3 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios fracción V, el bloqueo se dará únicamente después del cumplimiento de la finalidad con la que fueron recabados los datos personales hasta que cumpla el plazo de prescripción legal o contractual correspondiente, concluido éste se deberá proceder a la supresión en la base de datos, archivo, registro, expediente que corresponda, al mismo tiempo se está garantizando la supresión de los datos personales.

Los objetivos específicos para la supresión y borrado de datos personales son los siguientes:

- Que la supresión y borrado de los expedientes que contengan datos personales sea de forma legal.
- Que la supresión y borrado de los expedientes que contengan datos personales sea de forma operativa conforme a los procedimientos utilizados en el FIPRODEFO.
- Servir como base para el proceso adecuado de supresión y borrado de los expedientes que contengan datos personales.
- Guía para depuración de datos personales.

Este apartado es el conjunto de estructuras para el proceso de supresión y borrado de los expedientes que contengan datos personales en posesión del sujeto obligado; por lo tanto, los datos personales deberán estar contenidos en archivos apegados a un orden lógico y cronológico.

Bases para supresión y borrado seguro de archivos:

- Las bajas documentales se realizan mediante la aprobación del Grupo Interdisciplinario de Archivo.
- Los documentos físicos cuya baja ha sido procedente, se entregan a un reciclador, y estos serán vigilados por personal del FIPRODEFO hasta su destino final, en donde son triturados.

PLAN DE CONTINGENCIA

Ante la pérdida total o parcial de datos personales en posesión de este sujeto obligado, se debe contar con un plan de contingencia.

Con la evaluación de riesgos y la elaboración de las medidas de seguridad aplicables para prevenir las posibles vulneraciones a las que los datos personales se encuentran expuestos, el plan de contingencias de este sujeto obligado consiste en la aplicación de las medidas de seguridad tratadas en el apartado anterior, mismas que están sujetas a cambios por eventualidades no contempladas, por ello la importancia de señalar que el presente se trata de un plan de contingencia no limitativo.

Lo anterior, toda vez que en la actualidad existen cambios y grandes avances que van modificando la organización de la información, de igual manera no se está exento de nuevos riesgos a futuro.

Con la aplicación de las medidas de seguridad establecidas en este documento se buscan minimizar los riesgos o vulneraciones, pero a su vez se intenta propiciar el restablecimiento de los datos personales en el menor tiempo posible ante cualquier eventualidad.

En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada área administrativa en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo.

PLAN DE TRABAJO

La existencia del Documento de Seguridad, busca enmarcar los deberes del FIPRODEFO para la máxima protección de datos personales. Debido a la importancia y el contexto actual en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad de protección de datos personales.

La finalidad de este plan es plasmar de manera enunciativa, más no limitativa, las actividades que el FIPRODEFO realizará para la aplicación del presente documento de seguridad.

Lo anterior se realizará en base a las atribuciones establecidas en el la Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Jalisco y sus Municipios.

Para la ejecución del presente Documento de Seguridad, dentro de los 6 meses siguientes a la emisión del presente documento:

1. Se emitirá circular para difundir la emisión del presente documento, a través de la cual se remitirá copia digital del mismo a todos los correos institucionales vigentes.
2. Se comunicará a las áreas administrativas sobre la emisión del Documento de Seguridad, solicitando su apoyo para la difusión interna del mismo.
3. Se buscará la participación del ITEI para una primera capacitación básica para los empleados que recaban datos personales.

El Comité de Transparencia revisará de manera anual, a partir de la emisión del presente documento de seguridad:

1. Revisar lo concerniente al índice de Datos Personales y mantenerlo actualizado.
2. Actualizar las medidas de Seguridad conforme al Sistema de Protección de Datos Personales hecho para el FIPRODEFO
3. Actualizar el presente plan de trabajo.
4. Se emitirá un programa anual de capacitaciones y además se promoverá para que el personal del FIPRODEFO se mantenga capacitado no sólo por la Unidad de Transparencia del sujeto obligado, sino también mediante su asistencia a capacitaciones otorgadas por organismos competentes en la materia.

BIBLIOGRAFÍA

- Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus Municipios.
- Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.
- Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales https://www.gob.mx/cms/uploads/attachment/file/83122/MODELOS_Y_GU_AS_17-pdf
- GUIA PARA LA ELABORACIÓN DE UN DOCUMENTO DE SEGURIDAD V 1.4 https://www.ichitaip.org/infoweb/archivos/reader/pdp/Guia_elaboracion_Documento_seguridad.pdf
- Guía para elaborar un documento de seguridad. Formato guía para los sujetos obligados (ITEI) http://www.itei.org.mx/v3/documentos/guias/guia_documento_seguridad_so_31082018.pdf

Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco

El Fideicomiso para la Administración del Programa de Desarrollo Forestal del Estado de Jalisco, a través del Comité de Transparencia aprueba el presente Documento de Seguridad, el día 30 treinta de Agosto de 2019 dos mil diecinueve, lo anterior con fundamento en lo dispuesto por los artículos 3 fracción XIV, 5, 35, 36, 37, 38 y 39 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, así como los previstos en el artículo 3 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, y el artículo 28 del Código Civil del Estado de Jalisco.

Mtro. Arturo Pizano Portillo
Gerente del FIPRODEFO y
Presidente del Comité de Transparencia

Lic. Margarita Elizabeth Córdova Torres
Coordinadora Administrativa quien funge como
Órgano Interno de Control del Comité de Transparencia

Lic. Hugo Enrique Nolasco Reyes
Titular de la Unidad de Transparencia y
Secretario del Comité de Transparencia