**Documento de seguridad**

**COMISIÓN NACIONAL FORESTAL 2024**

**Contenido**

# Introducción……………………………………………………………………………………………………………………………………………...3

# I. El inventario de datos personales y de los sistemas de tratamiento……........................6

# II. Las funciones y obligaciones de las personas que traten datos personales………...8

# III, IV y V. Análisis de riesgos, Análisis de brecha, Plan de Trabajo………………………...………11

# VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad…………..19

# VII. El programa general de capacitación………………………………………………………………………….………21

# Actualización del documento de seguridad………………………………………………………………….………..22

# **Introducción.**

En los artículos 6 y 16 en su segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos, se fijan las bases para la creación de una Ley General en Materia de Protección de Datos personales, la cual se creó en enero de 2017; su aplicación y observancia es para todos los sujetos obligados en el ámbito federal, estatal y municipal. Asimismo, tendrá por objeto establecer, principios, bases y procedimientos para garantizar el derecho a toda persona a la protección de sus datos personales.

En concordancia, el artículo primero de la Ley General de Protección de Datos Personales en Posesión de Sujetos obligados, señala que son sujetos obligados, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos. De igual manera, los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.

En ese sentido, la Comisión Nacional Forestal, adquiere el carácter de responsable, por lo que deberá proteger los datos personales y los activos con los que cuente, con la finalidad de regular su tratamiento, garantizar que toda persona pueda ejercer el ejercicio de los derechos ARCO, así como promover y difundir una cultura de protección de datos personales.

Con respecto a lo establecido con el artículo 29 de la Ley General, la CONAFOR implementó mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en dicha Ley, así como en la Constitución y los Tratados Internacionales en los que el Estado mexicano es parte.

Asimismo, en enero de 2018, se publicaron los Lineamientos Generales de Protección de Datos Personales para el Sector Público, cuyo objetivo es desarrollar las disposiciones previstas en la Ley General de Datos y, con ello, hacer más comprensible el cumplimiento de los principios, deberes y obligaciones exigidos en materia de protección de datos personales.

Por consiguiente, dentro del Capítulo II de la Ley General, con relación al deber de seguridad, señala que los responsables, deberán establecer y mantener las medidas de seguridad en los siguientes términos: de carácter administrativo, físico y técnico para garantizar la protección de datos personales y salvaguardarlos de algún daño, perdida, alteración o destrucción, así como garantizar su confidencialidad e integridad.

En específico, el artículo 33 de la Ley General de Protección de Datos a la letra dice:

***“Artículo 33****. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*

***I. Crear políticas internas para la gestión y tratamiento de los datos personales,*** *que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;*

***II. Definir las funciones y obligaciones del personal*** *involucrado en el tratamiento de datos personales;*

***III. Elaborar un inventario de datos personales*** *y de los sistemas de tratamiento;*

***IV. Realizar un análisis de riesgo de los datos personales****, 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;***

***V. Realizar un análisis de brecha,*** *comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;*

***VI. Elaborar un plan de trabajo*** *para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;*

***VII. Monitorear y revisar de manera periódica las medidas de seguridad*** *implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y*

***VIII. Diseñar y aplicar diferentes niveles de capacitación del personal*** *bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.”*

Por lo tanto, las acciones realizadas con las medidas de seguridad para el tratamiento de los datos personales, fueron documentadas en un sistema de gestión, por lo que la CONAFOR creó un documento de seguridad de acuerdo a lo siguiente:

***“Artículo 35****. De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*

***I.*** *El inventario de datos personales y de los sistemas de tratamiento;*

***II.*** *Las funciones y obligaciones de las personas que traten datos personales;*

***III.*** *El análisis de riesgos;*

***IV.*** *El análisis de brecha;*

***V.*** *El plan de trabajo;*

***VI.*** *Los mecanismos de monitoreo y revisión de las medidas de seguridad, y*

***VII.*** *El programa general de capacitación.”*

El presente documento de seguridad será aplicable a las Unidades Administrativas de la Comisión Nacional Forestal, de acuerdo a su Estatuto Orgánico publicado en el Diario Oficial de la Federación el 30 de abril de 2021 y su reforma del día 16 de diciembre de 2022, publicada en dicho órgano de difusión.

Por todo lo anterior y en cumplimiento a las obligaciones antes descritas, el Comité de Transparencia, a través de su Unidad de Transparencia, presenta el documento de seguridad para que sea aprobado por el mismo.

MARCO NORMATIVO:

* Constitución Política de los Estados Unidos Mexicanos, artículo 6°, Base A y segundo párrafo del artículo 16.
* Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
* Ley Orgánica de la Administración Pública Federal.
* Lineamientos Generales de Protección de Datos Personales para el Sector Público.
* Lineamientos que establecen los parámetros, modalidades y procesamiento para la portabilidad de datos personales.
* Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
* Estatuto Orgánico de la CONAFOR

1. **El inventario de datos personales y de los sistemas de tratamiento.**

En relación con el artículo 33, fracción I y III de la Ley General, el cual establece que el responsable deberá mantener las medidas de seguridad para garantizar la protección de datos y al mismo tiempo crear políticas internas para la gestión y tratamiento de los mismos; la CONAFOR en concordancia con las unidades administrativas adscritas a la entidad, realizaron un diagnóstico, con la finalidad de establecer un inventario de los tratamientos de datos personales.

Asimismo, dentro del artículo 35 de la Ley General, se menciona que el inventario de datos personales y de los sistemas de su tratamiento, formará parte del documento de seguridad. De tal manera que en los Lineamientos Generales en los artículos 58 y 59, se establece lo siguiente:

***“Inventario de datos personales.”***

***“Artículo 58.*** *Con relación a lo dispuesto en el artículo 33, fracción III de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:*

1. *El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;*
2. *Las finalidades de cada tratamiento de datos personales;*
3. *El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;*
4. *El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;*
5. *La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;*
6. *En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y*
7. *En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.”*

***“Ciclo de vida de los datos personales en el inventario de éstos.”***

***“Artículo 59****. Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos generales, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:*

1. *La obtención de los datos personales;*
2. *El almacenamiento de los datos personales;*
3. *El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;*
4. *La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;*
5. *El bloqueo de los datos personales, en su caso, y*
6. *La cancelación, supresión o destrucción de los datos personales.*

*El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar.”*

A partir de lo anterior, la CONAFOR incorporó los inventarios de los distintos tratamientos de datos personales que realiza por cada unidad administrativa de la entidad, identificando los elementos informativos que señala el artículo 58 de los Lineamientos Generales y basados en el ciclo de vida de estos, como lo requiere el artículo 59 de los Lineamientos Generales.

Los inventarios forman parte integral del presente documento de seguridad y se encuentran contenidos en el Anexo 1.

# **II. Las funciones y obligaciones de las personas que traten datos personales.**

En relación al artículo 33, fracción II de la Ley General, el cual establece como una de las actividades a realizar por parte de los responsables, es la de definir las funciones y las obligaciones del personal involucrado en el tratamiento de datos personales, esto con la finalidad de implementar las actividades necesarias para mantener medidas de seguridad para garantizar la confidencialidad de los datos personales de acuerdo a lo siguiente:

* **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**.

***“Artículo 33.*** *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*

*(…)*

***II.*** *Definir las* ***funciones y obligaciones del personal involucrado*** *en el tratamiento de datos personales;”*

(…)

**Artículo 35.** *De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente*

*(…)*

***II.*** *Las* ***funciones y obligaciones*** *de las personas que traten datos personales;*

*(…)*

Asimismo, para efecto de establecer una organización dentro de la CONAFOR, y cumplir con los requisitos establecidos para delegar los roles y responsabilidades a las personas que traten con datos sobre el particular, se considera lo establecido en el artículo 57 de los Lineamientos Generales que señala lo siguiente:

* **Lineamientos Generales de Protección de Datos Personales para el Sector Público.**

***Funciones y obligaciones.***

***“Artículo 57.*** *Con relación a lo dispuesto en el artículo 33, fracción II de la Ley General, el responsable deberá* ***establecer y documentar***

***los roles y responsabilidades****, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.”*

*“El responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización,* ***conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión****, así como las consecuencias de su incumplimiento.”*

De acuerdo a lo anterior, y en cumplimiento a la normativa, este sujeto obligado, determina las funciones y obligaciones que deberán atender quienes conforme a sus atribuciones, realicen el tratamiento de datos personales de acuerdo a lo siguiente:

|  |  |
| --- | --- |
| **Funciones y obligaciones de las personas que traten datos personales.** | * Comunicar al personal de la CONAFOR el contenido del documento de seguridad. |
| * Establecer canales de comunicación con la Unidad de Transparencia, a fin de obtener asesoría u orientación sobre el tratamiento de datos personales que realiza. |
| * Observar los principios y deberes establecidos en la Ley de la materia para el adecuado tratamiento de los datos |
| * Velar por que se realice un adecuado tratamiento de los datos personales, conforme a los principios y deberes establecidos en la Ley. |
| * Proponer al responsable, la implementación y o actualización de medidas de seguridad, así como el desarrollo o adopción de esquemas de mejores prácticas, conforme a las disposiciones legales aplicables. |
| * Los servidores públicos deberán mantenerse actualizados en los cursos, talleres o programas de capacitación relacionados con la materia. |
| * Las áreas del responsable, deberán de remitir a la Unidad de Transparencia el inventario de tratamiento de datos personales, cuando esta lo solicite, se realice un nuevo tratamiento de datos o se actualicen las medidas de seguridad. |
| * Supervisar la implementación de medidas de seguridad para el tratamiento de datos. |
| * Utilizar los datos personales para la finalidad para la que fueron recabados |
| * Cumplir con las políticas de seguridad. |
| * Mantener la confidencialidad de la información |
| * Realiza altas y bajas de los usuarios del sistema |
| * Resguardar la información contenida |
| * Presentar su Acta de Entrega Recepción, por el término de su encargo, puesto o la entrega de bienes e información. |

Por otra parte, todo el personal que intervenga en el procesamiento y aprovechamiento de los datos personales deberán tratar únicamente los datos personales conforme a las instrucciones del responsable; abstenerse de tratar los datos para finalidades distintas a las instruidas por el responsable y finalmente, deberán guardar confidencialidad respecto de los datos personales tratados.

Estas obligaciones podrán ser modificadas por el Comité de Transparencia, a petición del servidor público responsable designado, conforme al art. 85 de la Ley General, salvaguardando en todo momento, el adecuado tratamiento de los datos personales al interior de la CONAFOR.

# **III, IV y V. Análisis de riesgos, análisis de brecha y Plan de Trabajo.**

**Análisis de Riesgos de la Comisión Nacional Forestal.**

El artículo 33, fracción IV de la Ley General, establece que unas de las medidas para mantener las medidas de seguridad y garantizar el derecho a la protección de datos personales, el responsable (Comisión Nacional Forestal) deberá realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento.

El objetivo de contar con un análisis de riesgos dentro de la CONAFOR será obtener un soporte a decisiones estratégicas para el apoyo en la definición y asignación efectiva de recursos, la justificación de esfuerzo en tiempo, los recursos humanos y financieros, así como la promoción de una mejora continua. Lo anterior para determinar con qué cuenta la organización en el tema de seguridad del tratamiento de los datos personales y poder estimar lo que podría pasar en caso de que algún activo resultase vulnerado.

En aras de cumplir con la normativa y el deber de seguridad que se encuentra establecido en la norma así como en el Programa de Protección de Datos Personales, la CONAFOR optó por apegarse a la metodología MAGERIT V3 para determinar el análisis de riesgo, y se consideraron los siguientes elementos:

1. **Activos.** Que se dividen en dos tipos:

**-De información:** Que hace referencia a los datos personales

**-De apoyo**: Son aquellos donde residen los activos de información (Hardware, Software, redes, telecomunicaciones, estructura organizacional, etc.)

1. **Amenazas**
2. **Vulnerabilidades**
3. Una vez que las áreas administrativas de la CONAFOR, integraron el inventario de datos personales correspondiente, se determinaron los activos relevantes, su interrelación y el valor de cada uno, lo anterior de la siguiente manera:

|  |  |
| --- | --- |
| TIPO DE ACTIVO |  |
| De Información | -Información personal definida en el contexto de la Ley Federal de Protección de Datos Personales en Posesión de los Sujetos Obligados. Adicionalmente podría ser considerado lo dispuesto en la materia por acuerdos internacionales, normatividad específica de la industria, o del giro particular del negocio, entre otros.  -Información estratégica, de alto costo o vital para alcanzar los objetivos determinados en el SGSDP, relacionada con el tratamiento de los datos personales.  -Procesos que son necesarios para cumplir con requerimientos contractuales, legales o regulatorios de la organización. |
| Hardware | -Servidores, estaciones de trabajo, computadoras de cualquier clase.  -Laptops, tablas, smartphones.  -Impresoras, copiadoras, escáner y teclado. |
| Soportes | -Discos ópticos (CD’s y DVDs), cintas magnéticas de audio, video y datos, fichas de microfilm, discos duros removibles, memorias USB, y demás medios de almacenamiento masivo no volátil. |
| Software | -CPU, memoria, discos, e interfaces de red, gestión de tareas o procesos, y servicios de gestión de permisos de usuario.  -Plataformas de actualización, antivirus empresariales.  -Administradores de bases de datos, mensajería instantánea, servidores web, editores de texto.  -Software comercial o diseñado in-house con el objetivo de ofrecer al usuario servicios y funciones específicas que apoyen en la operación del Sistema de Gestión de Datos Personales. |
| Redes y Telecomunicaciones | -Red Telefónica Pública Conmutada, Ethernet, Especificaciones de protocolos Wireless, Bluetooth. |
| Sitio | -Lugares que quedan fuera del alcance de la organización (vivienda del personal, hoteles, reuniones en otro lugar público).  -Oficinas, zonas de acceso restringido, zonas seguras.  -Suministro de agua, electricidad, aire acondicionado, manejo de desechos. |
| Personal y Entidad | -Custodios. Son aquéllos con responsabilidad funcional sobre los activos de información y de apoyo.  -Usuarios. Personas que utilizan los activos en el contexto de su actividad y quienes tienen responsabilidad específica al respecto (RH áreas financieras, gerentes).  -Personal Técnico. Personas a cargo de la operación, mantenimiento y desarrollo de los sistemas de información. Tienen privilegios de acceso o implementación especial para poder cumplir con sus tareas cotidianas (GTIC).  -Estructura de la organización. Está constituida por las diferentes ramas de la organización, incluyendo actividades multifuncionales de la administración (GRM)  -Proyectos o sistemas de la organización. Consiste en los grupos que surgen para determinados proyectos o servicios (Protección civil).  -Contratistas/ proveedores/ terceros. Son organizaciones ajenas que proveen con servicios o recursos a través de un contrato. Ejemplos: administración, almacenamiento de datos, consultores, servicios de soporte técnico de tecnología no propietaria |

1. Enseguida se proporcionó un valor a cada activo, esto para poder conocer el riesgo inherente de cada dato que conforma el sistema de tratamiento.
2. Se determinó el valor de cada activo en función de tres principios:

**-Confidencialidad:** ¿Qué importancia tendría el activo si fuera conocido por personas no autorizadas?

**-Integridad:** ¿Qué importancia tendría el activo si fuera alterado o modificado sin autorización o control?

**-Disponibilidad:** ¿Qué importancia tendría el activo si no estuviera disponible o accesible?

1. Para calcular el valor del activo: se sumaron los valores asignados a la confidencialidad, integridad y disponibilidad mediante la siguiente escala:

|  |  |
| --- | --- |
| Valor Cualitativo | Valor Cuantitativo |
| Bajo | 1-2 |
| Medio | 3-4 |
| Alto | 5-6 |

Una vez establecido el valor por cada propiedad de la seguridad de los datos, se obtuvo un valor único.

1. Enseguida se identificaron las **amenazas** que pudieran afectar a los activos, estas se terminaron por tres grupos:

-Deliberadas

-Ambientales

-Accidentales

1. El siguiente paso, fue estimar el riesgo con la siguiente formula:

**RIESGO= PROBABILIDAD X IMPACTO**

Para calcular el impacto (o consecuencias), se valoró en términos del costo derivado de los activos afectados, además se consideraron los daños producidos en el propio activo, lo siguiente:

* Daños personales
* Pérdidas financieras
* Interrupción de servicios
* Daño a la reputación

Por lo tanto, la estimación del grado de impacto se determinó mediante la aplicación de criterios en función de tres principios básicos se seguridad:

Confidencialidad, integridad y disponibilidad y será valorado en 5 escalas: 1 será muy bajo, 2 bajo, 3 medio, 4 alto y 5 muy alto y será establecido con la siguiente formula:

**IMPACTO TOTAL= CONFIDENCILIDAD + INTEGRIDAD + DISPONIBILIDAD**

**3**

|  |  |
| --- | --- |
| IMPACTO | |
| Valor cualitativo | Valor cuantitativo |
| Muy bajo | 1 |
| Bajo | 2 |
| Medio | 3 |
| Alto | 4 |
| Muy Alto | 5 |

Enseguida se calculó la probabilidad, ésta se refiere a la posibilidad de que un evento ocurra y la medida utilizada fue la siguiente:

|  |  |  |
| --- | --- | --- |
| **GRADO DE PROBABILIDAD** | | **CRITERIO** |
| Muy baja | 1 | No existe antecedente registrado en los últimos 10 años, y/o que por el entorno la posibilidad de que suceda sea mínima |
| Baja | 2 | Ha ocurrido un antecedente registrado en un período de 5 años, o que por el entorno y condiciones sea posible que ocurra |
| Media | 3 | Se ha presentado un antecedente registrado en un período anual y/o esporádicamente en intervalos de 3 a 5 años, o que por el tipo de entorno y condiciones sea posible que ocurra. |
| Alta | 4 | Han ocurrido más de dos eventos al término de un año, o bien que por las condiciones actuales o el tipo de entorno sea sumamente posible que suceda. |
| Muy Alta | 5 | Se ha presentado un evento en más de dos ocasiones en un período anual, y por las condiciones actuales o el tipo de entorno es muy probable que ocurran constantemente, quizá una vez al mes. |

El nivel de riesgo se presentó de manera cuantitativa y cualitativa, la escala se le fijó en 5 niveles en los que 1 es el riesgo muy bajo, 2 riesgo bajo, 3 riesgo medio, 4 alto y 5 muy alto. Para determinarlo se multiplicó el valor final del impacto por la probabilidad y el resultado se determinó mediante la siguiente tabla:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Muy alta-5 | 5 | 10 | 15 | 20 | 25 |
| Alta -4 | 4 | 8 | 12 | 16 | 20 |
| Media-3 | 3 | 6 | 9 | 12 | 15 |
| Baja-2 | 2 | 4 | 6 | 8 | 10 |
| Muy baja-1 | 1 | 2 | 3 | 4 | 5 |
|  | Insignificante-1 | Menor-2 | Crítico-3 | Grave-4 | Muy grave-5 |

**IMPACTO:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IMPACTO** | | **PROBABILIDAD** | | **NIVEL DE RIESGO** | |
| Cuantitativo | Cualitativo | Cuantitativo | Cualitativo | Cuantitativo | Cualitativo |
| 5 | Muy alto | 1 | Muy baja | 5 | Medio |
| 5 | Muy alto | 2 | Baja | 10 | Alto |
| 5 | Muy alto | 3 | Media | 15 | Alto |
| 5 | Muy alto | 4 | Alta | 20 | Muy alto |
| 5 | Muy alto | 5 | Muy alta | 25 | Muy alto |
| 4 | Alto | 1 | Muy baja | 4 | Bajo |
| 4 | Alto | 2 | Baja | 8 | Medio |
| 4 | Alto | 3 | Media | 12 | Alto |
| 4 | Alto | 4 | Alta | 16 | Alto |
| 4 | Alto | 5 | Muy alta | 20 | Muy alto |
| 3 | Medio | 1 | Muy baja | 3 | Bajo |
| 3 | Medio | 2 | Baja | 6 | Medio |
| 3 | Medio | 3 | Media | 9 | Medio |
| 3 | Medio | 4 | Alta | 12 | Alto |
| 3 | Medio | 5 | Muy alta | 15 | Alto |
| 2 | Bajo | 1 | Muy baja | 2 | Muy Bajo |
| 2 | Bajo | 2 | Baja | 4 | Bajo |
| 2 | Bajo | 3 | Media | 6 | Medio |
| 2 | Bajo | 4 | Alta | 8 | Medio |
| 2 | Bajo | 5 | Muy alta | 10 | Alto |
| 1 | Muy bajo | 1 | Muy baja | 1 | Muy Bajo |
| 1 | Muy bajo | 2 | Baja | 2 | Muy Bajo |
| 1 | Muy bajo | 3 | Media | 3 | Bajo |
| 1 | Muy bajo | 4 | Alta | 4 | Bajo |
| 1 | Muy bajo | 5 | Muy alta | 5 | Medio |

Finalmente, en caso de materializarse el riesgo en los activos, se determinaron los escenarios de vulneración y consecuencias para los titulares, teniendo como ejemplo los daños físicos en la persona y en su integridad, discriminación, daño moral, entre otros.

El resultado del Análisis de Riesgos por cada área administrativa de la Comisión Nacional Forestal, se encuentra contenido en el Anexo 2, sin embargo el mismo es clasificado como reservado.

**Análisis de brecha de la Comisión Nacional Forestal.**

En relación al artículo 33, fracción V de la Ley General, establece que unas de las medidas para mantener las medidas de seguridad y garantizar el derecho a la protección de datos personales, el responsable (Comisión Nacional Forestal) deberá realizar un análisis de brecha comparando las medidas de seguridad existentes contra las faltantes dentro de la institución, además de la existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

Por lo anterior, y una vez que la Comisión Nacional Forestal ha determinado el riesgo de cada tratamiento de los activos con los que cuenta cada área administrativa, se procedió a realizar el análisis de brecha determinando los controles que puedan proporcionar diversas opciones de tratamiento, tomando en cuenta lo siguiente:

1. Reducir el riesgo
2. Retener el riesgo
3. Evitar el riesgo
4. Compartir el riesgo
5. Aceptación del riesgo
6. Comunicación del riesgo

Dentro de la Unidad de Transparencia de la Comisión Nacional Forestal, ha implementado una escala basada en la metodología MAGERIT, para poder medir los aspectos organizativos de las áreas administrativas con la siguiente escala de madurez de los controles:

|  |  |  |  |
| --- | --- | --- | --- |
| FACTOR | NIVEL |  | CRITERIO |
| 0% | N0 | Inexistente | Inexistente |
|  | N1 | Inicial/ad hoc | Cuando se detecta un problema. No existe previsión. Es una medida reactiva. |
|  | N2 | Repetible pero intuitivo | Hay una persona que sin ser responsable, la realiza de forma preventiva y constante de acuerdo con su criterio. Tampoco está documentada. |
|  | N3 | Proceso definido | Está documentada. Tiene un responsable y está implementada. |
|  | N4 | Gestionado y medible | Además de estar documentada y funcionando, es medible. |
| 100% | N5 | Optimizado | Además de ser medible, está automatizada, y pueden saltar avisos cuando hay problemas en su implementación |

El Análisis de Brecha de cada activo, con la amenaza, el riesgo inherente, el control, la evidencia, el responsable y el nivel de madurez establecido con anterioridad por cada área administrativa de la CONAFOR, se encuentra contenido en el Anexo 3, sin embargo el mismo es clasificado como reservado.

**Plan de trabajo.**

Una vez que la CONAFOR determinó los resultados del análisis de riesgos y el análisis de brecha, se estipuló el plan de trabajo de conformidad al artículo 62 de los Lineamientos generales:

***“Artículo 62****. De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.*

*Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas faltantes.”*

Por lo anterior y una vez que fueron identificados los riesgos con los cuales se pueden ver comprometidos los datos personales y los objetos de tratamiento por parte de los sujetos responsables de la CONAFOR, los cuales se identificaron a través del análisis de brecha, las medidas de seguridad faltantes para cumplir con la correcta protección que conlleve a garantizar la seguridad y confidencialidad, se presentan las acciones a desarrollar, a través del Plan de Trabajo contenido en el Anexo 4, sin embargo el mismo es clasificado como reservado.

# **VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad.**

El artículo 33, fracción VII de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

Así, respecto a los mecanismos de monitoreo y revisión de las medidas de seguridad, el artículo 63 de los Lineamientos Generales señala lo siguiente:

***“Monitoreo y supervisión periódica de las medidas de seguridad implementadas***

***Artículo 63.*** *Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.*

*Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:*

*Los nuevos activos que se incluyan en la gestión de riesgos;*

*Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;*

*Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;*

*La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;*

*Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;*

*El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y*

*Los incidentes y vulneraciones de seguridad ocurridas”*

Mecanismos de Monitoreo

Se consideran los siguientes tipos de monitoreo:

1. Revisión de cumplimiento de las políticas relacionadas con el tratamiento de datos personales, a considerar:
2. Procesos involucrados en el tratamiento de datos personales.
3. Avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales.
4. Cambios en las amenazas, vulnerabilidades o impacto de los riesgos.
5. Sistemas de tratamiento para cumplir con los cambios normativos.
6. Revisión del riesgo, considerando el monitoreo de:
7. El entorno físico.
8. El entorno electrónico.
9. El plan de trabajo.
10. Actualización tecnológica.
11. Vulneraciones a la seguridad de los datos personales.

Monitoreo y supervisión periódica de las medidas de seguridad implementadas

La supervisión de las medidas de seguridad, se llevará a cabo conforme al Programa de revisiones administrativas y auditorías definido para cada año. Hasta el momento no se han realizado auditorías específicas en materia de protección de datos personales; sin embargo, se tiene contemplada la realización de una auditoría voluntaria en materia de protección de datos personales, al menos una vez al año conforme lo determine el en el Programa que determine el Comité de Transparencia.

# **VII. El programa general de capacitación.**

Con relación al programa de capacitación, el artículo 64 de los Lineamientos Generales señala que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Por su parte, el artículo 64 de los Lineamientos Generales señala lo siguiente:

***“Capacitación***

***Artículo 64****. Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.*

*En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, el responsable deberá tomar en cuenta lo siguiente:*

*Los requerimientos y actualizaciones del sistema de gestión;*

*La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;*

*Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y*

*Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.”*

A partir de lo anterior, la CONAFOR desarrolló su programa general de capacitación, mismo que integra el Anexo 5 de este documento de seguridad.

# **Actualización del documento de seguridad.**

El artículo 36 de la Ley General establece la obligación de la actualización del documento de seguridad cuando ocurran los siguientes eventos:

1. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
2. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
3. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
4. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En ese sentido, cada vez que se requiera actualizar alguno de los supuestos antes citados, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia con el objeto de que este determine si considera procedente la actualización del presente documento de seguridad.