FIRCO

FIDEICOMISO DE RIESGO COMPARTIDO

# DOCUMENTO DE SEGURIDAD

27 de agosto de 2024

**UNIDAD DE TRANSPARENCIA**

# Contenido

# GLOSARIO

**Áreas:** Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales.

**Autenticidad**: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

**Autentificar**: Acción de comprobar que la persona es quien dice ser. Ello, mediante el cotejo de uno o más datos en dicha identificación oficial contra (i) los datos en alguna otra identificación, documento, certificado digital (como el de la firma electrónica) o dispositivo que tenga la persona, (ii) los datos que sepa o tenga memorizados (su firma autógrafa o su contraseña, por ejemplo) o (iii) una o más características que coincidan con lo que es dicha persona (fotografía o huella dactilar, por ejemplo).

**Aviso de privacidad**: Documento a disposición del titular, generado en cualquier formato por el responsable durante la recuperación de datos, con el objeto de informarle los propósitos de su tratamiento.

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

**Bloqueo**: Identificación y conservación de datos personales una vez concluida la finalidad para la cual se recabaron, para determinar responsabilidades en relación con su tratamiento, hasta el plazo de su prescripción legal o contractual. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

**Ciclo de vida de la información:** Las etapas de la información desde su captación hasta su borrado o conservación

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

**Cómputo en la nube**: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

**Confiabilidad de la Información**: Expresa la garantía de que la información generada es adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

**Confidencialidad**: Propiedad de prevenir la divulgación de información a personas o sistemas no autorizados, y que garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma, es decir, asegurar que la misma no sea divulgada o accedida a personas o procesos no autorizados;

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

**Control de acceso**: Medida de seguridad que permite el acceso únicamente a quien está autorizado para ello y una vez que se ha cumplido con el procedimiento de identificación y autentificación;

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

**Datos personales sensibles**: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

**Derechos ARCO:** Hace referencia a las garantías constitucionales de acceso, rectificación, cancelación y oposición para el tratamiento de datos personales enunciadas en la LEY GENERAL DE DATOS.

**Destinatario(a):** Cualquier persona física o moral pública o privada que recibe datos personales;

**Disociación**: Procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura o contenido, su identificación.

**Documentos**: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico.

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

**Encargado(a):** La persona servidora pública o cualquier otra persona física o moral facultada por un instrumento jurídico o expresamente autorizado por el Responsable, para llevar a cabo el tratamiento físico o automatizado de los datos personales;

**Expediente**: Un conjunto de documentos.

**Evaluación del impacto en la protección de datos personales**: Documento mediante el cual los sujetos obligados valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

**Fuentes de acceso público**: Bases de datos, sistemas o archivos que, por disposición de ley, puedan ser consultadas públicamente cuando no exista impedimento por una

norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. -Excepto cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la LEY DE DATOS y demás normativa aplicable.

**Identificar**: Consiste aportar las pruebas necesarias para corroborar que una persona es quien dice ser, lo cual puede realizarse, por ejemplo, con una identificación que tenga validez oficial y en un ambiente electrónico con el nombre de usuario que se introduce al momento de ingresar al sistema (login).

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

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

**Medidas compensatorias**: Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios de comunicación masiva u otros de amplio alcance.

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

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

**Medidas de seguridad físicas**: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

**Medidas de seguridad técnicas**: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

**Organismo Garante**: Entidades con autonomía constitucional especializados en materia de acceso a la información y protección de datos personales. [En términos de los artículos 6o. y 116, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos].

**Persona Responsable**: La persona servidora pública titular de la unidad administrativa designada por el/la titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

**Personas Servidoras públicas**: Las mencionadas en el párrafo primero del Artículo 108 Constitucional y todas aquellas personas que manejen o apliquen recursos públicos federales.

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

**Responsable**: La persona servidora pública titular de la unidad administrativa designada por el/la titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

**Riesgo inherente**: Riesgo intrínseco al dato personal derivado del impacto negativo a la privacidad que puede causar en la persona

**RUSP**: Registro de Servidores Públicos del Gobierno Federal.

**Sistema de datos personales**: El conjunto ordenado de datos personales que estén en posesión de un sujeto obligado

**Sistema de Información**: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

**Sistema Nacional:** El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

**Soportes físicos**: Son los medios de almacenamiento identificables a simple vista, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados "a mano" o "a máquina", fotografías, placas radiológicas, carpetas, expedientes, entre otros.

**Supresión**: Baja archivística de los datos personales conforme a la normativa archivística aplicable; esto es, resultado de la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

**Tecnología de la Información:** Se refiere al hardware y software operado por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

**Titular**: Persona física a quien se refieren los datos personales que sean objeto de tratamiento.

**Transmisión de datos personales**: La entrega total o parcial de sistemas de datos personales a cualquier persona distinta del titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras o bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

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

**Transmisor**: Dependencia o entidad que posee los datos personales objeto de la transmisión.

**Tratamiento**: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración,

utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

**Unidades administrativas:** Las que, de acuerdo con la estructura orgánica del FIRCO, y demás normatividad aplicable, tengan la información de conformidad con las facultades que les y que puedan contar, dar tratamiento y ser responsables de los datos personales.

**Unidad de Transparencia**: Instancia a la que hace referencia el artículo 45 de la LGTAIP.

**Usuario/a:** Persona facultada por un instrumento jurídico o expresamente autorizado por el responsable que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin posibilidad de agregar o modificar su contenido.

## PRESENTACIÓN

El 1 de junio de 2009, se publicó en el Diario Oficial de la Federación el Decreto por el que se adiciona un segundo párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) con la siguiente disposición.:

*"Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley. La ley determinará las excepciones a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas, o para proteger los derechos de terceros."*

Con esta reforma, se instauró el derecho fundamental a la protección de los datos personales, incluyendo los derechos correlativos de acceso, rectificación, cancelación y oposición en relación con el manejo de los datos por parte de cualquier entidad o persona, ya sea pública o privada, que tenga acceso o disponga de los datos personales de las personas.

Esta iniciativa que tuvo por objeto desarrollar en el máximo nivel de nuestra normatividad, el derecho a la protección de datos personales, aplicables tanto al sector público como al privado.

El 7 de febrero de 2014, se publicó en el Diario Oficial de la Federación el Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia

De lo anterior se promulgaron diversas disposiciones tales como:

- Ley General de Transparencia y Acceso a información Pública (LGTAIP)
- Ley General de Transparencia y Acceso a información Pública (LGTAIP)
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LEY DE DATOS), promulgada en México el 26 de enero de 2017. Ésta última con los siguientes objetivos:

De esta última se destacan sus principales objetivos:

a) Garantizar el Derecho a la Protección de Datos Personales: Establecer y proteger el derecho fundamental de los individuos a la protección de sus datos personales

en posesión de cualquier autoridad, entidad u organismo público, asegurando su manejo adecuado y el respeto a su privacidad.

b) Desarrollar Principios y Obligaciones: Elaborar y definir los principios, deberes y obligaciones que deben cumplir los responsables del tratamiento de datos personales, así como las entidades públicas que los gestionan. Esto incluye asegurar que los datos sean tratados de manera legal, adecuada y proporcional.

c) Regulación de Tratamiento y Portabilidad de Datos: Establecer bases mínimas y condiciones homogéneas para el tratamiento y la portabilidad de los datos personales, garantizando que estos procesos se realicen de manera segura y conforme a la ley.

d) Facilitar el Ejercicio de Derechos: Regular el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los titulares de datos personales, permitiendo a los individuos controlar cómo se utilizan sus datos personales.

e) Distribuir Competencias: Asignar competencias y responsabilidades entre los organismos garantes a nivel federal y en las entidades federativas para asegurar la implementación y supervisión de las disposiciones de la ley.

f) Promover la Transparencia y Rendición de Cuentas: Fomentar la transparencia en el manejo de datos personales por parte de los sujetos obligados y garantizar la rendición de cuentas respecto al cumplimiento de las obligaciones establecidas en la ley.

g) Establecer Procedimientos de Supervisión y Control: Crear mecanismos para la supervisión y control de las prácticas de tratamiento de datos personales, asegurando que las entidades públicas implementen medidas de seguridad adecuadas y cumplan con las disposiciones legales.

h) Promover la Cultura de Protección de Datos: Incentivar la formación y sensibilización sobre la protección de datos personales tanto en las entidades públicas como en los ciudadanos, promoviendo una cultura de respeto y protección de la privacidad.

Estos objetivos buscan asegurar que los datos personales en posesión de los sujetos obligados sean manejados de manera segura, protegiéndolos contra daño, perdida, alteración, destrucción, uso, acceso o tratamiento no autorizado, en apego a los principios de protección de datos establecidos por la normatividad en la materia.

La LEY DE DATOS establece como *datos personales* cualquier información concerniente a una persona física identificada o identificable, y se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Asimismo, hace la distinción entre los datos personales sensibles, los cuales son definidos como aquellos que se refieran a los aspectos más íntimos de una persona, o cuya utilización indebida puede dar lugar a actos de discriminación o a riesgos graves para éste. Estos pueden ser: origen racial o étnico, estado de salud actual o futura, información

genética, creencias religiosas, filosóficas o morales, así como opiniones de carácter político preferencias sexuales, por mencionar algunos.

Con la publicación de la LEY DE DATOS, y posteriormente con la publicación de los *"Lineamientos Generales de Protección de Datos Personales para el Sector Público Federal"*, emitidos por el INAI y publicados en el Diario Oficial de la Federación el 26 de enero de 2018; todas las dependencias y entidades, como Sujetos Obligados y en su carácter de Responsables, deberán llevar a cabo el tratamiento de datos personales de personas físicas, con finalidades concretas y conforme a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; y deberán adoptar medidas de seguridad en atención a los sistemas de datos que traten en el ámbito de sus facultades y atribuciones que la normatividad aplicable le confiera,

Por lo anterior se debe elaborar un documento que integre el inventario de datos personales, los sistemas de su tratamiento, las funciones y obligaciones de las personas que efectúen dicho tratamiento, el análisis de riesgo, el análisis de brecha, el plan de trabajo, los mecanismos de monitoreo y revisión de las medidas de seguridad y el programa general de capacitación. A este documento se le denomina *Documento de Seguridad para la Protección de Datos Personales*.

Es importante destacar que la coordinación y supervisión para la elaboración del Documento de Seguridad, es responsabilidad de las Unidades de Transparencia dentro de las entidades y dependencias del sector público, asegurándose que se elabore conforme a la normativa vigente y que se actualice periódicamente.

Asimismo, será el Responsable de Protección de Datos Personales dentro de cada una de las áreas del Sujeto Obligado que da tratamiento a datos personales, quien tenga la función y obligación de la elaboración, implementa y mantenimiento del Documento de Seguridad;

En este orden de ideas y en cumplimiento del deber de seguridad que establece la Ley de Datos, se elaboró el presente Documento de Seguridad, donde se definen las medidas de seguridad técnicas, físicas y administrativas a adoptar por el Responsable, para garantizar la confidencialidad, integridad y disponibilidad de la información personal que el Fideicomiso de Riesgo Compartido posee

En función de ello, el Fideicomiso de Riesgo Compartido presenta el *Documento de Seguridad* que atiende los procesos en los que intervienen datos personales.

El Documento está integrado por los apartados:

i. Inventario de datos personales y sus sistemas de tratamiento;
ii. Las funciones y obligaciones de las personas que tratan datos personales;
iii. Resultados del Análisis de riesgos;
iv. Resultados del Análisis de brecha;
v. Plan de trabajo para atender los hallazgos;
vi. Mecanismos de monitoreo y revisión de las medidas de seguridad; y
vii. Programa general de capacitación

Para la elaboración del presente Documento de Seguridad se llevaron a cabo las siguientes fases:

**Primera fase:** se llevó a cabo la identificación de información que involucran datos personales en las Unidades Administrativas del FIRCO, la persona responsable y los procesos a su cargo.

**Segunda fase:** Identificación del flujo de los datos personales, dividiéndose en 5 etapas:

- Paso 1. Identificación de datos personales
- Paso 2. Identificación de mecanismos de obtención de datos personales
- Paso 3. Identificación de medios de almacenamiento
- Paso 4. Identificación de permisos y tratamiento
- Paso 5. Identificación del ciclo de vida de los datos personales

Se identificaron los datos personales que componen las bases o expedientes, su clasificación, el tipo, el personal que tiene acceso, los permisos otorgados y sus funciones y obligaciones, así como identificar y documentar el ciclo de vida de los datos personales.

**Tercera fase:** Evaluación de medidas de seguridad cuya finalidad fue la gestión del riesgo para identificar e implementar medidas de seguridad adecuadas a la categoría del dato personal para proteger los datos personales de una vulneración.

Lo anterior a través de:

a) Análisis de brecha. Se identificaron medidas de seguridad físicas, técnicas y administrativas existentes, faltantes, o, en su caso, el reforzamiento de las actuales.
b) Análisis de riesgos de datos personales y privacidad. Se identificaron los riesgos derivados del tratamiento de datos personales al que están expuestos los datos de este tipo, en cada etapa de su ciclo de vida, para posterior implementación o adecuación de las medidas de protección o controles, y comprender los impactos de situaciones temidas o no deseadas

**Cuarta fase:** Plan de Trabajo. En esta fase se determinaron las acciones a realizar para la gestión del riesgo, a través de la implementación de las medidas de seguridad faltantes, las que serán sustituidas o reforzadas, con base en los resultados de la Tercera fase.

**Quinta Fase:** Mecanismos de Monitoreo y revisión de las medidas de seguridad que permitirá verificar la seguridad en el tratamiento de los datos personales durante todo su ciclo de vida.

**Sexta Fase:** Programa de capacitación general.

El contenido del presente documento incluye los conceptos básicos en la materia, así como los resultados específicos del FIRCO..

# MARCO NORMATIVO.

- Constitución Política de los Estados Unidos Mexicanos (Artículos 6 y 16, párrafo II)
- Ley General de Transparencia y Acceso a la Información Pública (Títulos Sexto y Séptimo).

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Título I Capítulo II, Titulo Segundo. Título Tercero, Capítulo I y II)
- Ley General de Responsabilidades Administrativas
- Ley Orgánica de la Administración Pública Federal
- Ley General de Archivos
- Guía para cumplir con los principios y deberes de la Ley General de Protección
- de Datos Personales en Posesión de Sujetos Obligados.
- Ley Federal de Transparencia y Acceso a la Información Pública (Título Quinto; artículos 11, fracción VI; 16 y 113, fracción I).
- Ley Federal de Responsabilidades Administrativas de los Servidores Públicos
- Lineamientos Generales de Protección de Datos Personales para el Sector Público (Titulo Primero. Capítulo II; Título Segundo. Capítulo II).
- Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales
- Lineamientos Comité de Transparencia
- Guía de Apoyo para la Elaboración del Documento de Seguridad v1.4. emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos-Personales (INAI).
- Guía de Borrado Seguro. Editada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).
- Metodología de Análisis de Riesgo BAA.

# DOCUMENTO DE SEGURIDAD

## 1. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

Con el fin de garantizar el cumplimiento de las obligaciones establecidas en los artículos 33, fracción III y 35, fracción I de la LEY DE DATOS, el FIRCO llevo a cabo la elaboración del Inventario de Tratamiento de Datos Personales correspondientes a las Unidades Administrativas que manejan este tipo de información.

Entendiendo como Inventario de Tratamiento, el control documentado que se lleva de los tratamientos que realizan las Unidades Administrativas de los datos personales conforme al tipo (sensibles o no), cuantos y cuales sistemas de datos se tienen y en qué soportes se almacena o guarda la información (documento físico o formato electrónico).

Para la conformación de este Inventario las personas servidoras públicas designadas como Responsables de dicha información consideran lo siguiente:

1. **¿Qué tratamientos de datos personales realiza la unidad administrativa?**

Las personas servidoras públicas deberán de identificar cada uno de los procesos en los que la Unidad Administrativa trata datos personales en el marco de sus competencias y facultades para atender un trámite.

Se deberán enlistar los tipos de tratamientos y cada uno de los datos personales que son usados para ello.

2. **¿Qué persona o unidad administrativa está a cargo de estos procesos y que por tanto sea la administradora de las bases de datos o archivos que se generen con motivo de dichos tratamientos?**

Se identificará y definirá si la unidad administrativa está a cargo del proceso en donde se tratan los datos personales, según las atribuciones o facultades normativas, además de las personas servidoras públicas que tienen acceso al tratamiento.

3. **¿Qué es un tratamiento de datos personales?**

Conforme al Artículo 3, fracción XXXIII de la LEY DE DATOS, un tratamiento es cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Una vez que la Unidades Administrativas hayan identificado los tratamientos de los cuales estén a cargo, será necesario determinar lo siguiente, conforme al ciclo de vida de los datos personales:

**a) ¿Cómo se obtienen los datos personales?**

Se debe de especificar de donde se obtienen los datos personales:

- Directamente del titular.
  - De manera personal, con la presencia física del titular de los datos personales o su representante.
  - Vía telefónica.
  - Por correo electrónico.
  - Por Internet o sistema informático.
  - Por escrito presentado directamente en las oficinas del sujeto obligado.
  - Por escrito enviado por mensajería.
- Mediante una transferencia
  - Quién transfiere los datos personales y para qué fines
  - Medios por los que se realiza la transferencia
- De una fuente de acceso público

**b) ¿Qué tipo de datos personales se tratan? ¿Son sensibles?**

Se deberá elaborar un listado de los datos personales que se recaban y utilizan en el tratamiento de datos personales, identificando si se trata de datos personales sensibles o no, conforme a la diferenciación que marca el artículo III de la LEY DE DATOS.

Categorías de datos personales y sus niveles:

- **Datos identificativos:** Nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Clave de elector, Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía y otros.
- **Datos electrónicos:** Direcciones electrónicas, tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona, para su

identificación en Internet, acceso a sistemas de información u otra red de comunicaciones electrónicas

- **Datos laborales:** Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio entre otros.
- **Datos académicos:** Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos y demás información.
- **Datos de salud:** El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona.
- **Datos patrimoniales:** Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales.
- **Datos sobre procedimiento administrativos**: La 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, fiscal, administrativa o de cualquier otra rama del Derecho.
- **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria.
- **Datos biométricos:** huellas dactilares, ADN, geometría de la mano, características de iris y retina y demás análogos.
- **Datos sensibles:** origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas, la pertenencia a sindicatos, la salud y preferencia sexual.
- **Datos personales de naturaleza pública**: Aquellos que por mandato legal sean accesibles al público.

**c) ¿Dónde son almacenados los datos personales?**

Es importante incluir en el Inventario de Tratamientos, el formato en que se almacenan los datos personales, así como la ubicación de dichos archivos tomando en cuenta lo siguiente:

Formato en que se encuentra la información: Físico y/o Electrónico
Ubicación de la información (si es en físico ubicar sección, serie y subserie de los archivos).

**d) ¿Para qué finalidad se utilizan los datos personales?**

Las finalidades son acciones más específicas de los procesos de los que derivan los tratamientos de datos personales. En este punto, es necesario identificar cada una de las finalidades concretas para las cuales se tratan los datos personales, lo cual se vincula de manera directa con las actividades en las que se utilizan datos personales, por ejemplo, nómina o expediente de personal, tramites o servicios que realizan las dependencias o sujetos obligados, recursos de revisión.

Es necesario identificar si se requiere el consentimiento (tácito o expreso) y en caso de no requerirse, definir qué supuestos (fracciones) del artículo 22 de la LEY DE DATOS se actualizan. Asimismo, se deberá señalar el marco jurídico que da facultades para el tratamiento de datos personales (disposición normativa, artículo, fracción, inciso, párrafo).

**e) ¿Quién tiene acceso a la base de datos o archivo (sistemas de tratamiento) y a quién se le comunican los datos personales al interior del sujeto obligado?**

Se deberá identificar el catálogo de personas servidoras públicas al interior de la Unidad Administrativa del FIRCO, que tienen acceso a los datos personales y para qué fin.

**f) ¿Intervienen encargados en el tratamiento de los datos personales?**

Es necesario identificar si las bases de datos son manejadas por un encargado a nombre del área o de la propia institución, y se debe identificar el instrumento por el que dicha relación jurídica se sustenta.

Es necesario identificar el nombre del encargado y el número de contrato, pedido o convenio correspondiente.

Por ENCARGADO se debe de entender a la persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trate datos personales a nombre y por cuenta del responsable. Por ejemplo, una empresa que se encargue de manejar una base de datos para brindar un software de seguridad a nombre del área, pero no que no implica la transferencia de datos personales.

**g) ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?**

Partiendo de la definición de Transferencia, como toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o encargado.

Por lo anterior es necesario identificar las autoridades o externos da la institución a quienes se comunican datos personales y los fines de transferencia.

Para llevar a cabo dicha transferencia es importante señalar si se requiere el consentimiento para la transferencia, el tipo de consentimiento que se requiere en su caso (tácito o expreso y por escrito), y en caso de que no se requiera el consentimiento, se deberá definir qué supuestos (fracciones) de los artículos 22, 66 o 70 de la LEY DE DATOS se actualizan.

**h) ¿Se difunden los datos personales?**

Hay que señalar si los datos personales se difunden y el fundamento jurídico para ello.

**i) ¿Cuál es el plazo de conservación de los datos personales?**

Este plazo tendría que estar definido en los instrumentos de clasificación archivística, por lo que es necesario identificar a qué serie documental pertenecen los archivos o bases de datos en los que están contenidos los datos personales.

**j) ¿Cómo se suprimen los datos personales?**

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos previo bloqueo en su caso.

Las personas servidoras públicas deberán de adoptar medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, esto es,

políticas, métodos y técnicas orientadas a la supresión definitiva de éstos, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.

Se deberán de considerar los siguientes atributos y los medios de almacenamiento, físicos y/o electrónicos en los que se encuentren los datos personales:

- **Irreversibilidad**: Que el proceso utilizado no permita recuperar los datos personales.
- **Seguridad y confidencialidad:** Que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la Ley General y los Lineamientos Generales.
- **Favorable al medio ambiente**: Que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.

Una vez que concluya el plazo de conservación de estos, no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

En este contexto y conforme a los artículos 58 y 59 de los Lineamientos, el FIRCO llevó a cabo la elaboración de los inventarios de tratamientos de datos personales del FIRCO que integran la siguiente información:

i. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;
ii. Las finalidades de cada tratamiento de datos personales;
iii. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;
iv. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;
v. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;
vi. 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,
vii. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.
viii. Ciclo de vida de los datos personales en el inventario de éstos
ix. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
x. El bloqueo de los datos personales, en su caso, y
xi. La cancelación, supresión o destrucción de los datos personales.

Estos Inventarios son documentos actualizables en caso de que se identifiquen nuevos tratamientos de datos personales o se supriman los que se encuentran identificados actualmente.

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

A continuación, se enlistan los Inventarios elaborados en el FIRCO:

AGRICULTURA

FIDEICOMISO DE RIESGO COMPARTIDO

INVENTARIO DE TRATAMIENTOS DE DATOS PERSONALES

FIRCO
FIDEICOMISO DE RIESGO COMPARTIDO

| NOMBRE DEL INVENTARIO DE TRATAMIENTO | CLAVE DE INVENTARIO | UNIDAD ADMINISTRATIVA | SIGLAS | CATEGORÍA DE DATOS PERSONALES RECABADOS | DATOS PERSONALES SENSIBLES |
|---|---|---|---|---|---|
| **ACCEDER A APOYOS E INCENTIVOS DE PROGRAMAS/ PROYECTOS/ COMPONENTES** | DS-2024-DEM-01 | **Dirección Ejecutiva de Microcuencas- Gerencia de Desarrollo Regional** | **DEM** | Identificación<br>Electrónicos<br>Financieros<br>Patrimoniales | Origen étnico o racial<br>Estrato económico |
| **EXPEDIENTE PERSONAL** | DS-2024-SgP-02 | **Dirección Ejecutiva de Administración y Finanzas- Gerencia de Administración- Subgerencia de Personal** | **SgP** | Identificación<br>Financieros<br>Laborales<br>Electrónicos<br>Patrimoniales<br>Académicos<br>Movimientos migratorios<br>Salud<br>Biométricos | Biométricos |
| **PROVEEDORES DE BIENES Y SERVICIOS** | DS-2024-SgRMSG-03 | **Dirección Ejecutiva de Administración y Finanzas- Gerencia de Administración- Subgerencia de Recursos Materiales y Servicios Generales** | **SgRMS** | Identificación<br>Electrónicos<br>Laborales<br>Financieros<br>Patrimoniales | No |
| **VIÁTICOS Y PASAJES PARA ATENCIÓN DE COMISIONES** | DS-2024-SGRMSG-04 | **Dirección Ejecutiva de Administración y Finanzas- Gerencia de Administración- Subgerencia de Recursos Materiales y Servicios Generales** | **SgRMS** | Identificación<br>Laborales<br>Financieros<br>Electrónicos | No |
| **PROCEDIMIENTOS DE ACCESO A INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES** | DS-2024-UT-05 | **Dirección de Análisis y Servicios Institucionales- Gerencia de Planeación- Unidad de Transparencia** | **UT** | Identificación<br>Electrónicos | No |

## 2. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS SERVIDORAS PUBLICAS QUE TRATAN DATOS PERSONALES.

En el Inventario de tratamiento de datos personales se encuentran identificadas las funciones de las personas servidoras públicas que intervienen en el tratamiento de datos personales del FIRCO.

Adicional a ellas y con fundamentado en el Artículo 33 fracción II de la LEY DE DATOS, toda vez que las personas servidoras públicas del Fideicomiso que en el ejercicio de sus atribuciones traten datos personales, deben garantizar la confidencialidad, integridad y disponibilidad de los mismos, se identificaron las siguientes funciones y obligaciones conforme al rol que desempeñan en el tratamiento de datos personales:

| ROL | PERSONA SERVIDORA PUBLICA | FUNCIONES COMUNES | FUNCIONES ESPECÍFICAS |
|---|---|---|---|
| **Responsable** | Siempre será el titular de la Unidad Administrativa donde se traten los datos personales. | • Observar los principios de legalidad, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de información que contenga datos personales<br>• Utilizar únicamente los datos personales necesarios, relevantes y adecuados para la finalidad de su tratamiento y conforme a sus facultades<br>• Evitar obtener y tratar datos personales, a través de métodos engañosos o fraudulentos.<br>• Atender los mecanismos para asegurar que los datos personales a los que tengan acceso conforme al ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen<br>• Mantener exactos, completos, correctos y actualizados los datos personales para garantizar la veracidad de los mismos<br>• Observar permanentemente las medidas de seguridad de carácter administrativo, físico y técnico necesarias para la protección de los datos personales evitando daño, perdida, alteración, destrucción o uso, acceso o tratamiento no autorizado<br>• Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones<br>• Suprimir, previo bloqueo, los datos personales una vez que hayan dejado de ser necesarios para los fines especificados en el aviso de privacidad y al término del período de conservación<br>• Implementar medidas de seguridad administrativas, físicas y técnicas para proteger los datos personales contra daños, pérdidas, alteraciones, destrucción, acceso no | • Dar aviso a la Unidad de Transparencia de los Sistemas que involucren tratamiento de datos personales, a cargo de dicha Unidad Administrativa<br>• Validar que la información entregada por los titulares de los datos personales, sea la estrictamente necesaria para cumplir con los fines legales para los cuales se hubieran recabado<br>• Conocer el Inventario de tratamiento de datos personales y por cada uno, conocer el tipo de datos personales que se recaban.<br>• Dar seguimiento a las acciones de capacitación para los servidores públicos involucrados en el tratamiento de los datos personales<br>• Verificar regularmente que los avisos de privacidad, así como el inventario de datos personales se encuentren actualizados<br>• Mantener actualizada la relación de usuarios que traten datos personales<br>• Informar al titular a través del aviso de privacidad, que deberá difundirse por medios electrónicos y físicos, sobre la existencia, características principales y finalidades del tratamiento de sus datos personales<br>• Notificar a la Unidad de Transparencia cualquier vulneración de seguridad relacionada con las bases de datos personales en su custodia<br>• Llevar un registro de los hechos cuando se presente algún incidente de |

| | | | |
|---|---|---|---|
| | | autorizado, y garantizar su confidencialidad, integridad y disponibilidad<br>• Evitar la transferencia de datos personales sin el consentimiento de las personas titulares, y cuando se actualice alguna de las excepciones previstas en la LEY DE DATOS.<br>• Atender de manera pronta y expedita en los plazos establecidos, las solicitudes de ejercicio de los derechos ARCO<br>• Dar aviso a los superiores jerárquicos, ante cualquier acción que pueda poner en riesgo los datos personales, y en general que puedan vulnerar la seguridad de los datos personales<br>• Estar capacitado en materia de tratamiento de datos personales<br>• Atender a los requerimientos de información que solicite la Unidad de Transparencia | vulneración de seguridad de los datos personales |
| **Administrador** | Persona servidora pública designada de manera expresa el Titular de la Unidad Administrativa que tiene a su cargo la responsabilidad de la administración de los datos y/o sistemas y de los operadores. | | • Mantener actualizado el Sistema<br>• Determinar los servidores públicos que deben tener acceso a los datos personales en función del tratamiento que debe aplicarse a los mismos.<br>• Autorizar los accesos de los servidores públicos, determinar los privilegios y limitantes y llevar un registro de los mismos<br>• Implementar las medidas de seguridad con la finalidad de evitar vulneraciones de la información |
| **Usuarios** | Persona servidora pública autorizada por el responsable para dar tratamiento y/o tenga acceso a los datos y/o sistemas de datos personales. | | • Sus funciones quedan determinadas de acuerdo al perfil que se haya asignado en el tratamiento de los datos personales de cada uno de los sistemas |

Es importante resaltar que en el momento de la elaboración del presente documento en el FIRCO no existen las figuras de “Oficial de Datos Personales” ni de “Encargado” que surge del servicio que implica la trasferencia de datos para su tratamiento, por lo que, en el momento en que existan se atenderá lo previsto en el artículo 59 de la LEY DE DATOS y los artículos correspondientes de los Lineamientos Generales.

Las funciones y obligaciones de las personas que tratan datos personales forman parte integral del Documento de Seguridad, y se encuentra integradas en el **Anexo 2.**

## 3. ANÁLISIS DE RIESGOS

Los datos personales a los que tienen acceso las personas servidoras públicas del FIRCO en el ejercicio de sus atribuciones, se manipulan y resguardan de manera física y electrónica, según las actividades para las cuales se lleva a cabo el tratamiento.

Con la realización del Análisis de Riesgos Institucionales se lograron identificar los riesgos inherentes y los riesgos latentes de cada uno de los tratamientos de datos personales y permitió conocer el nivel de riesgo para cada uno de los tratamientos.

A partir del resultado del análisis de riesgos el FIRCO se están determinando los controles a implementar para su protección, junto con como las medidas de seguridad, buscando asegurar un alto nivel de protección para todos los datos personales, para evitar cualquier

vulneración que pueda tener consecuencias negativas para los titulares de los datos, como es la divulgación de información o los daños a su vida privada, moral o patrimonial.

Se extrae de este análisis que para los datos personales que se almacenan físicamente, los riesgos incluyen la pérdida, el uso indebido, el deterioro por negligencia o la destrucción principalmente.

En cuanto a los datos personales almacenados electrónicamente, los riesgos inherentes son el uso indebido de la información y posibles fallas en los equipos o sistemas.

Por lo anterior y de conformidad con el Artículo 35 de la LEY DE DATOS, el Análisis de Riesgo de los tratamientos de Datos Personales del FIRCO, forma parte del presente documento, identificándose como **Anexo 3.**

## 4. ANÁLISIS DE BRECHA

El **Análisis de Brecha** de datos personales identifica las medidas de seguridad existentes, en su caso, y las que son necesarias para la seguridad de los datos personales. Este análisis es fundamental en cualquier programa de protección de datos personales, ya que permite identificar las medidas de seguridad implementadas y evaluar su eficacia en el tratamiento de los riesgos.

Una brecha de seguridad es un incidente de seguridad que afecta a datos de carácter personal, ya sea tratados digitalmente o en formato papel. Este incidente puede tener un origen accidental o intencionado y puede producirse cuando un intruso logra sortear los mecanismos de seguridad.

Para poder considerar que existen *medidas de seguridad* para la protección de los datos personales en posesión del FIRCO, estas deben identificarse y determinar el grado de desarrollo que mantiene a través de la revisión de las siguientes características

i. Que se encuentren documentadas
ii. Que se encuentren implementadas
iii. Que generen registros de su operación
iv. Que existan métricas que permitan dar seguimiento a su eficacia
v. Que existan reportes dirigidos a los Titulares de las unidades administrativas para la toma de decisiones
vi. Que existan acciones que permitan incrementar su eficacia

Actualmente las únicas medias de seguridad implementadas en el FIRCO, que impactan de manera directa en la protección de datos personales, las que se encuentran contenidas en el MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN V.3 de la Gerencia de Servicios de Comunicaciones y Sistemas del FIRCO.

Dentro de las medidas de seguridad que pueden ser consideradas para la protección de los tratamientos de datos personales en el FIRCO se encuentran las siguientes:

**A. MEDIDAS FÍSICAS:**

- Revisión de la ubicación donde se almacenan los datos personales y valorar la implementación de medidas de protección como cámaras de seguridad y cerraduras para controlar el acceso

**B. MEDIDAS ADMINISTRATIVAS**

- Establecer deberes y responsabilidades claros para las personas servidoras públicas involucrados en el uso y protección de datos personales
- Se establecen procedimientos para mantener un registro físico de los servidores públicos que tienen acceso a los datos personales y de los datos contenidos en los documentos.
- Incluir mayor número de cursos centrados en la protección de datos personales en el Programa de Capacitación Anual del FIRCO
- Designar al responsable para la gestión y rendición de cuentas en cuanto a la protección de datos personales, asegurando el cumplimiento de la legislación y las políticas de seguridad
- Se establecen procedimientos para mantener un registro físico de los servidores públicos que tienen acceso a los datos personales y de los datos contenidos en los documentos.

**C. MEDIDAS TECNOLÓGICAS**

- Implementar nuevas tecnologías o programas para enfrentar futuras amenazas en el área de ciberseguridad

De conformidad con el Artículo 35 de la LEY DE DATOS, el Análisis de Brecha de los tratamientos de Datos Personales del FIRCO, forma parte del presente documento y se encuentra en el **Anexo 4.**

## 5. PLAN DE TRABAJO

De acuerdo con los artículos 33, fracción VI y 35, fracción V de la Ley General de Protección de Dato Personales en Posesión de Sujetos Obligados, y 62 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el FIRCO elaboró el Plan de Trabajo 2024-2026 a fin de implementar de las medidas de seguridad requeridas conforme a los resultados obtenidos del Análisis de Riesgos y del Análisis de Brecha

El Plan de Trabajo conforme a lo establecido en el Documento de Seguridad de datos personales es fundamental por varias razones clave:

1) Cumplimiento Normativo: Asegura que el FIRCO cumpla con las leyes y regulaciones vigentes en materia de protección de datos personales, evitando sanciones legales y reputacionales.
2) Protección de la Información: Establece medidas y protocolos para proteger los datos personales contra accesos no autorizados, pérdida, destrucción o alteración, garantizando la confidencialidad, integridad y disponibilidad de la información.
3) Confianza de los Usuarios: Fortalece la confianza de los titulares de datos personales, ciudadanos, cliente, en el FIRCO al demostrar un compromiso sólido con la seguridad de sus datos personales.
4) Prevención de Incidentes: Ayuda a identificar y mitigar riesgos potenciales relacionados con la seguridad de datos, reduciendo la probabilidad de incidentes de seguridad y sus consecuencias.
5) Planificación y Organización: Facilita una planificación estructurada y la implementación de medidas de seguridad efectivas, asegurando que se aborden todas las áreas críticas y se asignen recursos adecuados.
6) Respuesta a Incidentes: Incluye estrategias y procedimientos para la gestión y respuesta a incidentes de seguridad, minimizando el impacto de cualquier brecha de seguridad y asegurando una rápida recuperación.
7) Capacitación: Promueve la capacitación continua del personal en materia de seguridad de datos, fomentando una cultura organizacional orientada a la protección de la información.
8) Evaluación y Mejora Continua: Permite la evaluación regular de las prácticas de seguridad y la implementación de mejoras continuas, adaptándose a nuevos riesgos y cambios en el entorno de la protección de datos.

   En resumen, un plan de trabajo de seguridad de datos personales es crucial para garantizar que se implementen las medidas necesarias para proteger la información, cumpliendo con las obligaciones legales y fortaleciendo la confianza en la organización.

El Plan de Trabajo elaborado por la Unidad de Transparencia forma parte sustantiva del Documento de Seguridad y se identifica como el **Anexo 5.** del mismo.

## 6. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDA DE SEGURIDAD

- Como un mecanismo de monitoreo, la Unidad de Transparencia rendirá informes semestrales al Comité de Transparencia en los que dé cuenta del avance de cumplimiento del Plan de Trabajo, así como de las novedades o cuestiones adicionales que estime conveniente hacer de su conocimiento.
- 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;

- Revisión de cumplimiento de las políticas internas relacionadas con el tratamiento de datos personales a fin de asegurar que las personas servidoras públicas realicen los tratamientos de datos personales en concordancia con lo dispuesto en la Ley de Datos, los Lineamientos Generales, y demás normatividad que resulte aplicable.
- Revisará y, en su caso, actualizará los procesos involucrados en el tratamiento de datos personales.
- Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales.
- Revisión del riesgo. Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales

| ELEMENTO A REVISAR | FUNDAMENTO | ACCIONES |
|---|---|---|
| **NUEVOS ACTIVOS QUE SE INCLUYAN EN LA GESTIÓN DE RIESGOS;** | 63, fracción I, de los Lineamientos Generales | Revisión del cumplimiento de la normatividad aplicable al tratamiento de los datos personales. |
| **MODIFICACIONES NECESARIAS A LOS ACTIVOS, COMO PODRÍA SER EL CAMBIO O MIGRACIÓN TECNOLÓGICA, ENTRE OTRAS** | 63, fracción II, de los Lineamientos Generales | Revisión del cumplimiento de la normatividad aplicable al tratamiento de los datos personales. |
| **LAS NUEVAS AMENAZAS QUE PODRÍAN ESTAR ACTIVAS DENTRO Y FUERA DE SU ORGANIZACIÓN Y QUE NO HAN SIDO VALORADAS** | 63, fracción III, de los Lineamientos Generales | Revisión del cumplimiento de la normatividad aplicable al tratamiento de los datos personales<br>Revisión del Riesgo: Monitoreo del entorno físico y electrónico |
| **POSIBILIDAD DE QUE VULNERABILIDADES NUEVAS O INCREMENTADAS SEAN EXPLOTADAS POR LAS AMENAZAS CORRESPONDIENTES** | 63, fracción IV, de los Lineamientos Generales | Revisión del cumplimiento de la normatividad aplicable al tratamiento de los datos personales<br>Revisión del Riesgo: Monitoreo del entorno físico y electrónico |
| **VULNERABILIDADES IDENTIFICADAS PARA DETERMINAR AQUÉLLAS EXPUESTAS A AMENAZAS NUEVAS O PASADAS QUE VUELVAN A SURGIR** | 63, fracción V, de los Lineamientos Generales | Revisión del cumplimiento de la normatividad aplicable al tratamiento de los datos personales<br>Revisión del Riesgo: Monitoreo del entorno físico y electrónico |
| **CAMBIO EN EL IMPACTO O CONSECUENCIAS DE AMENAZAS VALORADAS, VULNERABILIDADES Y RIESGOS EN CONJUNTO, QUE RESULTEN EN UN NIVEL INACEPTABLE DE RIESGO** | 63, fracción VI, de los Lineamientos Generales | Revisión del cumplimiento de la normatividad aplicable al tratamiento de los datos personales<br>Actualización del Plan de Trabajo y revisión de avances |
| **INCIDENTES Y VULNERACIONES DE SEGURIDAD OCURRIDAS** | 63, fracción VII, de los Lineamientos Generales | Revisión del cumplimiento de la normatividad aplicable al tratamiento de los datos personales<br>Vulneraciones a la seguridad de datos personales. |

## 7. PROGRAMA DE CAPACITACIÓN

La capacitación en un sistema de gestión de protección de datos personales es crucial por varias razones, dado el papel fundamental que juega en la seguridad y conformidad con las normativas. A continuación, se detallan los aspectos clave de su importancia:

1. El cumplimiento legal y normativo.
2. Cumplimiento Legal y Normativo
3. Protección de Datos Personales
4. Crear conciencia y responsabilidad
5. Mejora Continua
6. Capacitación Práctica
7. Simulaciones y Ejercicios.
8. Preparación para Auditorías y Revisiones

En resumen, la capacitación es esencial para garantizar que todos los servidores públicos del FIRCO entiendan y apliquen correctamente las políticas y procedimientos de protección de datos personales, ayudando a proteger la información sensible, cumplir con las normativas, y mantener la confianza pública de protección de datos personales que son necesarios para cualquier servidor público

El **Programa de Capacitación** en Materia de datos personales se encuentra como Anexo **Anexo 6** del Documento de Seguridad.

## 8. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

Con base en el artículo 36 de la LEY DE DATOS, se actualizará el Documento de Seguridad cuando ocurran las siguientes acciones:

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

| FECHA DE ACTUALIZACIÓN | MOTIVO DE LA ACTUALIZACIÓN |
|---|---|
| **27/08/2024** | Aprobación del Documento de Seguridad del FIRCO |

ANEXO 1 Inventario de Tratamientos de Datos Personales

ANEXO 2 Funciones y obligaciones

ANEXO 3 Análisis de Riesgo

ANEXO 4 Análisis de Brecha

ANEXO 5 Plan de Trabajo

ANEXO 6 Programa de capacitación