INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Guía para la elaboración de un Documento de seguridad v1.4

Agosto 2016

Guía para la elaboración de un Documento de seguridad v1.4

Tabla de contenido

Notas de versiones

Versión Agosto 2016. Respecto a la versión anterior (Julio 2009), se actualizó el nombre, logotipo y siglas del Instituto, debido al cambio de naturaleza jurídica del antes Instituto Federal de Acceso a la Información Pública (IFAI), por el ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Asimismo, se eliminó de la carátula del documento el nombre de la Dirección General de Clasificación y Datos Personales, debido a que dicha Dirección ya no existe en la actual estructura del INAI. De manera adicional, se actualizaron los hipervínculos a los documentos referidos.

Introducción

En toda organización, la información es un activo que, al igual que sus instalaciones, capital humano y recursos financieros, debe protegerse mediante un conjunto coherente de procesos y sistemas diseñados, administrados y mantenidos por la propia organización.

De esta manera, la gestión de la seguridad de la información, como parte de un sistema administrativo más amplio, busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información, aplicando un enfoque basado en los riesgos que la organización afronta.

Para lograr lo anterior, es necesario llevar a cabo una correcta administración de riesgos a fin de que éstos puedan ser asumidos, mitigados, transferidos o evitados de manera eficiente, sistemática y estructurada, que se adapte a los cambios que se produzcan en el entorno y en la información.

Es justamente el avance vertiginoso de las tecnologías de la información el que posibilita la recolección y almacenamiento de grandes volúmenes de información en pequeños dispositivos y facilita su transmisión por medios remotos a grandes distancias en cuestión de segundos. Lo anterior incluye el tratamiento de información relativa o concerniente a personas físicas, cuya protección es una atribución del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en su calidad de órgano garante de la protección de datos personales en el ámbito del Poder Ejecutivo Federal.

En la Administración Pública Federal el riesgo de sufrir la pérdida de información personal, sea ésta producto de la voluntad de un agente pernicioso o bien resultado del caso fortuito, siempre está presente. Las vulneraciones de seguridad generan altos costos institucionales además de afectaciones en la esfera de otros derechos y libertades fundamentales de las personas (por ejemplo, el acceso no autorizado a información del estado de salud de un individuo por personas ajenas al tratamiento de dicho paciente).

Es por ello que **no** resulta conveniente escatimar recursos y esfuerzos en el establecimiento de controles para la protección de la información frente a acciones o situaciones no deseadas, pues de esa manera, además de garantizar la continuidad de la operación de los sujetos obligados, se protege a los individuos a los que se refiere dicha información.

A efecto de que las dependencias y entidades de la Administración Pública Federal puedan conocer el tipo de controles a que se refiere el párrafo anterior, éstos deben estar documentados y ser difundidos para el conocimiento de todos los involucrados en el tratamiento de la información.

Al respecto, el Trigésimo tercero de los Lineamientos establece la obligación de que las dependencias y entidades expidan un documento de seguridad que contenga las medidas de seguridad administrativa, física y técnica aplicables a la protección de sistemas de datos personales, ya que dejar constancia por escrito de dichas medidas de seguridad permite identificar los roles, actividades y responsabilidades de los servidores públicos o terceros contratados que dan tratamiento a información personal, así como una ágil verificación de los controles implementados para el aseguramiento de ésta.

Por lo anterior, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, conforme la facultad prevista en el artículo 37, fracción IX de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, pone a su disposición la presente **Guía para la elaboración de un Documento de seguridad** que tiene por objeto garantizar en la Administración Pública Federal la correcta documentación de los controles de seguridad mínimos indispensables que deben considerarse según lo previsto en el Trigésimo cuarto de los Lineamientos.

El modelo propuesto en esta Guía no es limitativo. Los sujetos obligados, tomando en cuenta factores como el tamaño y estructura de la organización, objetivos, clasificación de la información, requerimientos de seguridad y procesos, entre otros aspectos relativos a su contexto, pueden prever y aplicar medidas de seguridad adicionales —como aquellas que desde 1980 han trascendido para conformar el estándar internacional en materia de seguridad de la información ISO/IEC 27002:2005 (anterior ISO/IEC 17799:2005)—, lo cual se determina en razón de los activos que poseen los sujetos obligados y los riesgos a los que dichos activos están expuestos.

En ese sentido, el modelo que se presenta pretende brindar a las dependencias y entidades homogeneidad en la redacción, organización y contenido para que los Comités de Información, conjuntamente con el área de tecnologías de la información y los responsables de los sistemas de datos personales, elaboren su propio Documento de seguridad en el que describan las medidas de seguridad administrativa, física y técnica implementadas para la protección de los sistemas de datos personales que custodian.

1. Terminología

1.1. Abreviaturas

APF Administración Pública Federal.
DOF Diario Oficial de la Federación.
INAI Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
LFTAIPG Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

1.2. Conceptos básicos

Para la aplicación de la Guía para la elaboración de un Documento de seguridad —en adelante Guía—, se deberán considerar las definiciones contenidas en los artículos 3 de la LFTAIPG[1] y 2 de su Reglamento[2]; así como lo previsto en el Tercero de los Lineamientos de Protección de Datos Personales[3] —en adelante Lineamientos—, las Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales[4] —en adelante Recomendaciones— y los conceptos que se señalan en el presente apartado.

1.2.1. Documento de seguridad

Concepto

Documento elaborado por el sujeto obligado que contiene las medidas de seguridad administrativa, física y técnica aplicables a sus sistemas de datos personales con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen. El documento tiene como propósito identificar el universo de sistemas de datos personales que posee cada dependencia o entidad, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

Dicho documento deberá mantenerse siempre actualizado y ser de observancia obligatoria para todos los servidores públicos de las dependencias y entidades, así como para las personas externas que debido a la presentación de un servicio tengan acceso a tales sistemas o al sitio donde se ubican los mismos.

Marco jurídico

El Capítulo V de los Lineamientos establece un conjunto mínimo de medidas de seguridad que cada dependencia o entidad deberá considerar al perfilar su estrategia de seguridad para la protección de los datos personales bajo su custodia, según el tipo de soportes —físicos, electrónicos o ambos— en los que residen dichos datos y dependiendo del nivel de protección que tales datos requieran —bajo, medio o alto— conforme a la naturaleza de los mismos.

---

1 Publicada en el DOF el 11 de junio de 2002, disponible en http://www.dof.gob.mx/nota_detalle.php?codigo=727870&fecha=11/06/2002
2 Publicado en el DOF el 11 de junio de 2003 disponible en http://inicio.ifai.org.mx/MarcoNormativoDocumentos/ReglamentoLFTAIPG_11062003.pdf
3 Publicados en el DOF el 30 de septiembre de 2005, disponibles en http://inicio.inai.org.mx/MarcoNormativoDocumentos/lineamientos_protdaper.pdf
4 Disponibles en http://inicio.ifai.org.mx/Estudios/estudio41.pdf

En el mismo sentido, el Trigésimo tercero de los Lineamientos establece que las dependencias y entidades deberán expedir un Documento de seguridad que contenga las medidas administrativas, físicas y técnicas aplicables a los sistemas de datos personales y que dicho documento será de observancia obligatoria.

En cuanto al **contenido mínimo del Documento de seguridad**, el Trigésimo cuarto de los Lineamientos señala lo siguiente:

> " […]
>
> **Requisitos del documento de seguridad**
>
> **Trigésimo cuarto.** El documento mencionado en el Lineamiento anterior deberá contener, como mínimo, los siguientes aspectos:
>
> I. El nombre, cargo y adscripción de los Responsables, Encargados y Usuarios;
> II. Estructura y descripción de los sistemas de datos personales;
> III. Especificación detallada del tipo de datos personales contenidos en el sistema;
> IV. Funciones y obligaciones de los servidores públicos autorizados para acceder al sitio seguro y para el tratamiento de datos personales;
> V. Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido en los presentes Lineamientos, las cuales deberán incluir lo siguiente:
>
> a) Procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja usuarios y claves de acceso para la operación del Sistema de datos personales;
> b) Actualización de información contenida en el Sistema de datos personales;
> c) Procedimientos de creación de copias de respaldo y de recuperación de los datos;
> d) Bitácoras de acciones llevadas a cabo en el Sistema de datos personales;
> e) Procedimiento de notificación, gestión y respuesta ante incidentes; y
> f) Procedimiento para la cancelación de un Sistema de datos personales.
>
> […] "

1.2.2. Tipos de seguridad: administrativa, física y técnica

Es importante aclarar las diferencias que existen entre las medidas de seguridad administrativa, física y técnica para que el sujeto obligado cuente con estos elementos teóricos al momento de elaborar su Documento de seguridad. A continuación se agrupan los temas que corresponden a cada tipo de seguridad tomando como base el estándar internacional ISO/IEC 27002:2005 que se refiere a mejores prácticas sobre seguridad de la información:

a) Las **medidas de seguridad administrativa** son aquellas que deben implementarse para la consecución de los objetivos contemplados en los siguientes apartados:

- **Política de seguridad.** Definición de directrices estratégicas en materia de seguridad de activos, alineadas a las atribuciones de las dependencias o entidades. Incluye la elaboración y emisión interna de políticas, entre otros documentos regulatorios del sujeto obligado.
- **Cumplimiento de la normatividad.** Los controles establecidos para evitar violaciones de la normatividad vigente, obligaciones contractuales o la política de seguridad interna. Abarca, entre otros, la identificación y el cumplimiento de requerimientos tales como la legislación aplicable al

sujeto obligado, los derechos de propiedad intelectual, la protección de datos personales y la privacidad de la información personal.

- **Organización de la seguridad de la información.** Establecimiento de controles internos y externos a través de los cuales se gestione la seguridad de activos. Considera, entre otros aspectos, la organización interna, que a su vez se refiere al compromiso de la alta dirección y la designación de responsables, entre otros objetivos; asimismo, considera aspectos externos como la identificación de riesgos relacionados con terceros.
- **Clasificación y control de activos.** Establecimiento de controles en materia de identificación, inventario, clasificación y valuación de activos conforme a la normatividad aplicable.
- **Seguridad relacionada a los recursos humanos.** Controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral.
- **Administración de incidentes.** Implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información. Incluye temas como el reporte de eventos y debilidades de seguridad de la información.
- **Continuidad de las operaciones.** Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información. Incluye planeación, implementación, prueba y mejora del plan de continuidad de la operación del sujeto obligado.

b) Las **medidas de seguridad física** atañen a las acciones que deben implementarse para contar con:

- **Seguridad física y ambiental.** Establecimiento de controles relacionados con los perímetros de seguridad física y el entorno ambiental de los activos, con el fin de prevenir accesos no autorizados, daños, robo, entre otras amenazas. Se enfoca en aspectos tales como los controles implementados para espacios seguros y seguridad del equipo.

c) Las medidas de **seguridad técnica** son las aplicables a sistemas de datos personales en soportes electrónicos, servicios e infraestructura de telecomunicaciones y tecnologías de la información, entre otras, se prevén las siguientes acciones:

- **Gestión de comunicaciones y operaciones.** Establecimiento de controles orientados a definir la operación correcta y segura de los medios de procesamiento de información, tanto para la gestión interna como la que se lleva a cabo con terceros. Incluye, entre otros aspectos, protección contra código malicioso y móvil, copias de seguridad, gestión de la seguridad de redes y manejo de medios de almacenamiento.
- **Control de acceso.** Establecimiento de medidas para controlar el acceso a la información, activos e instalaciones por parte de los responsables autorizados para tal fin, considerando en ello, la protección contra la divulgación no autorizada de información. Abarca, entre otros temas, gestión de acceso de los usuarios, control de acceso a redes, control de acceso a sistemas operativos y control de acceso a las aplicaciones y a la información.
- **Adquisición, desarrollo, uso y mantenimiento de sistemas de información.** Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y mantenimiento, hasta su cancelación o baja definitiva. Considera procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros.

1.2.3. Tipo de soportes: físicos y electrónicos

Es importante explicar la diferencia entre un soporte físico y un soporte electrónico debido a que las medidas de seguridad que el sujeto obligado implemente para cada sistema de datos personales están estrechamente relacionadas con el tipo de soportes utilizados.

Para lograr lo anterior, es preciso referirse a las definiciones que se prevén en las Recomendaciones emitidas por el Instituto:

- **Soportes físicos.** Son los medios de almacenamiento inteligibles a simple vista, es decir, 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.

- **Soportes electrónicos.** Son los medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil.

El Decimoséptimo y el Trigésimo de los Lineamientos hacen mención de los conceptos arriba señalados cuando se alude a los tipos de soportes, medios de almacenamiento o formatos —físicos o electrónicos— en los cuales residen los datos personales del sistema que custodia el sujeto obligado.

Una vez explicado lo anterior, es preciso señalar que el sujeto obligado deberá identificar el tipo de soporte en el que residen los datos personales de cada uno de los sistemas que posee con el propósito de corroborar que las medidas de seguridad implementadas sean aplicables a cada caso. Por tanto, en el Documento de seguridad deberá constar si los datos personales del sistema residen en:

i) Soporte físico;
ii) Soporte electrónico, o
iii) Ambos tipos de soportes.

1.2.4. Nivel de protección que requieren los datos personales

Para que el sujeto obligado pueda identificar las medidas de seguridad que resultan aplicables a cada uno de sus sistemas, debe considerar el tipo de datos personales que contiene, lo cual determina el nivel de protección requerido: básico, medio o alto, como a continuación se señala:[5]

1. **Nivel de protección básico**:

   a) **Datos de identificación**: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.
   b) **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.

[5] Ver inciso II de las *Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales.*

2. Nivel de protección medio:

a) **Datos patrimoniales**: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.
b) **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales**: Información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.
c) **Datos académicos**: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.
d) **Datos de transito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

3. Nivel de protección alto:

a) **Datos ideológicos**: Creencia religiosa, ideología, afiliación política y sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros.
b) **Datos de salud**: Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros.
c) **Características personales**: Tipo de sangre, ADN, huella dactilar u otros análogos.
d) **Características físicas**: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.
e) **Vida sexual**: Preferencia sexual, hábitos sexuales, entre otros.
f) **Origen**: Étnico y racial.

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

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

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

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

1.2.5. Tipo de transmisiones de datos personales y Modalidades para la transmisión

Una transmisión de datos personales implica 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.[6]

[6] Lineamiento Tercero, fracción VI de los Lineamientos de Protección de Datos Personales.

En el ámbito de la APF, existen tres **tipos de transmisiones** que se pueden llevar a cabo dependiendo de quién sea el destinatario:

a) **Interinstitucionales:** Transmisiones de datos a dependencias y entidades de la APF, entidades federativas y municipios;
b) **Internacionales:** Transmisiones a gobiernos u organismos internacionales, y
c) **Con entes privados u organizaciones civiles públicas o privadas**.

Para implementar las medidas de seguridad aplicables a las transmisiones citadas, debe considerarse la **modalidad por la cual se envían los datos personales a los destinatarios**, pudiendo hacerse mediante el traslado de soportes físicos, mediante el traslado físico de soportes electrónicos o el traslado sobre redes electrónicas. Cada una de estas modalidades se caracteriza por lo siguiente:

a) **Traslado de soportes físicos**: En esta modalidad los datos personales se trasladan en medios de almacenamiento inteligibles a simple vista que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos. Ejemplo del traslado de soportes físicos es cuando una dependencia envía por correspondencia oficios o formularios impresos.

b) **Traslado físico de soportes electrónicos:** En esta modalidad se trasladan físicamente para entregar al destinatario los datos personales en archivos electrónicos contenidos en medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos. Ejemplo de ello es cuando una dependencia entrega a otra por mensajería oficial un archivo electrónico con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB, entre otros.

c) **Traslado sobre redes electrónicas**: En esta modalidad se transmiten los datos personales en archivos electrónicos mediante una red electrónica. Por ejemplo, cuando un archivo electrónico con un listado de beneficiarios se envía de una dependencia a otra por Internet.

1.2.6. Diferencias entre identificar, autenticar y autorizar en el control de acceso

El control de acceso es una 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 autenticación. En ese sentido, cabe precisar el significado de los siguientes conceptos:

a) **Identificar** consiste en tomar conocimiento de que una persona es quien dice ser. Lo anterior se logra, 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*).

b) **Autentificar** (o autenticar) a una persona se refiere a comprobar que esa persona es quien dice ser. Ello se logra cuando se cotejan 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).

c) **Autorizar** se refiere al acceso que se le permite a la persona que se ha identificado y autenticado apropiadamente. Esto depende del o de los permisos que le conceda el responsable de autorizar los accesos.

Es importante que el sujeto obligado identifique las diferencias entre estos conceptos pues cada uno de ellos implica la implementación de medidas de seguridad distintas pero relacionadas entre sí. Ejemplo de lo anterior es cuando se implementan medidas de seguridad en capas en el control de acceso, como las siguientes:

a) Mostrar una identificación oficial para acceder a las instalaciones del sujeto obligado en un punto de revisión —control de acceso en el perímetro exterior—.
b) Una vez adentro de sus instalaciones, una segunda capa de protección se establece cuando el sujeto obligado implementa un control biométrico de huella dactilar para autenticar a la persona que fue identificada en el perímetro exterior y de este modo pueda ingresar al almacén donde se archivan los soportes físicos o el centro de datos donde residen soportes electrónicos —control de acceso en el perímetro interior—.
c) Finalmente, la persona previamente identificada y autenticada, ingresa al sistema, a través de un usuario y contraseña, para realizar consultas en el mismo, pues el responsable autorizó el acceso con permiso de "solo lectura".

2. Objetivos

2.1. Objetivo general

Proporcionar a las dependencias y entidades de la Administración Pública Federal los elementos mínimos con los que debe contar un Documento de seguridad.

2.2. Objetivos específicos

- Explicar los conceptos que el sujeto obligado debe tomar en cuenta para la elaboración de su Documento de seguridad.
- Orientar a los sujetos obligados respecto de las medidas de seguridad administrativa, física y técnica mínimas con las que debe contar un Documento de seguridad, según lo previsto en el Trigésimo cuarto de los Lineamientos.
- Ofrecer una guía y un modelo para la creación de dicho documento.

3. Modelo de Documento de seguridad

Considerando que el Lineamiento Trigésimo Tercero del Capítulo V, "Documento de seguridad", señala que las dependencias y entidades, a través de su Comité de Información, conjuntamente con el área de tecnología de la información, informática o su equivalente, expedirán un documento que contenga las medidas administrativas, físicas y técnicas de seguridad aplicables a los sistemas de datos personales; el INAI presenta el siguiente modelo tan solo como una referencia para el desarrollo del documento de seguridad que cada sujeto obligado debe realizar, pues deben considerarse para su elaboración las particularidades de cada sistema de datos personales, la estrategia de seguridad establecida y los riesgos que afronta cada dependencia o entidad.

El presente Modelo de Documento de seguridad para los Sistemas de Datos Personales se ha generado a partir de lo dispuesto en los Lineamientos de Protección de Datos Personales y las Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales emitidos por el INAI e indica,

conforme dichas disposiciones, las medidas de seguridad mínimas recomendadas para coadyuvar al cumplimiento relacionado con la integridad, confidencialidad y disponibilidad de la información.

Es importante señalar que el formato y la estructura del modelo pueden variar y que no es un modelo limitativo, sino que se pretende presentar únicamente los contenidos mínimos de un Documento de seguridad conforme lo prevé la normatividad y las mejores prácticas internacionales en la materia.

Idealmente, el sujeto obligado debe elaborar un Documento de seguridad en el que incluya todos los sistemas de datos personales bajo su custodia. No obstante, también es posible que elabore un Documento de seguridad por unidad administrativa en el que se incluyan los sistemas que opera y custodia cada una. Finalmente, la tercera opción es elaborar un documento de seguridad para cada sistema que posee el sujeto obligado.

El esquema elegido para el modelo de Documento de seguridad que aquí se presenta es el que contiene todos los sistemas de datos personales que posee y custodia el sujeto obligado, organizados por unidad administrativa.

Es recomendable que el sujeto obligado analice y documente las medidas de seguridad aplicables a cada uno de sus sistemas de datos personales considerando los ejemplos y explicaciones contenidas en las notas al pie del modelo, y sustituya con su información el texto que se encuentra en *cursivas* o en corchetes.

Finalmente, es importante recordar al sujeto obligado que el Documento de seguridad tiene el carácter de información reservada, de conformidad con el Vigésimo noveno de los Lineamientos de Protección de Datos Personales, por lo que deberá incluir la leyenda de clasificación correspondiente en el mismo.

DOCUMENTO DE SEGURIDAD DE [*DENOMINACIÓN DEL SUJETO OBLIGADO*]

PARTE 1. CATÁLOGO DE SISTEMAS DE DATOS PERSONALES

A. *[Denominación de la Unidad administrativa A]*

A1. [*Nombre del sistema A1]*

Responsable:

- Nombre:
- Cargo:
- Funciones: *[Descripción de las atribuciones con relación al tratamiento de los datos personales sistema]*
- Obligaciones: *[Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema]*

Encargados:[7]

- Nombre: *[Nombre del Encargado 1]*
- Cargo:
- Funciones:
- Obligaciones:

- Nombre: *[Nombre del Encargado 2]*
- Cargo:
- Funciones:
- Obligaciones:

Usuarios:[8]

- Nombre: *[Nombre del Usuario 1]*
- Cargo:
- Funciones:
- Obligaciones:

- Nombre: *[Nombre del Usuario 2]*
- Cargo:
- Funciones:
- Obligaciones:

- Nombre: *[Nombre del Usuario 3]*
- Cargo:
- Funciones:

7 Se tienen que poner los datos de todos los Encargados del sistema.
8 En caso de ser muchos usuarios, se recomienda agregar la información como Anexo al Documento de Seguridad.

- Obligaciones:

Folio de registro en el Sistema Persona:

Datos personales contenidos en el sistema:
[Señalar el tipo de dato personales que contiene el sistema, además de listar cada uno de los datos personales recabados][9]

A2. *[Nombre del sistema A2]*

Responsable:

- Nombre:
- Cargo:
- Funciones:
- Obligaciones:

Encargados:

- Nombre: *[Nombre del Encargado 1]*
- Cargo
- Funciones:
- Obligaciones:

- Nombre: *[Nombre del Encargado 2]*
- Cargo
- Funciones:
- Obligaciones:

Usuarios:

- Nombre: *[Nombre del Usuario 1]*
- Cargo:
- Funciones:
- Obligaciones:

- Nombre: *[Nombre del Usuario 2]*
- Cargo:
- Funciones:
- Obligaciones:

- Nombre: *[Nombre del Usuario 3]*
- Cargo:

[9] Ejemplo:
Datos de identificación (nombres, apellido paterno, apellido materno, domicilio, estado civil)
Datos laborales (correo electrónico institucional y teléfono institucional)

- Funciones:
- Obligaciones:

Folio de registro en el Sistema Persona:

Datos personales contenidos en el sistema:

B. [Denominación de la unidad administrativa B]

B1. [*Nombre del sistema B1]*

Responsable:

- Nombre:
- Cargo:
- Funciones:
- Obligaciones:

Encargados:

- Nombre: *[Nombre del Encargado 1]*
- Cargo
- Funciones:
- Obligaciones:

- Nombre: *[Nombre del Encargado 2]*
- Cargo
- Funciones:
- Obligaciones:

Usuarios:

- Nombre: *[Nombre del Usuario 1]*
- Cargo:
- Funciones:
- Obligaciones:

- Nombre: *[Nombre del Usuario 2]*
- Cargo:
- Funciones:
- Obligaciones:

Folio de registro en el Sistema Persona:

Datos personales contenidos en el sistema:

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

A1. *[Nombre del sistema A1]*

1. **Tipo de soporte:** [10]

   a) Tipo de soporte:[11]
   b) Descripción:[12]

2. **Características del lugar donde se resguardan los soportes**:

   [Describir el lugar en el que físicamente se encuentran los soportes del sistema][13]

A2. *[Nombre del sistema A2]*

1. **Tipo de soporte:**

   a) Tipo de soporte
   b) Descripción:

2. **Características del lugar donde se resguardan los soportes:**[14]

B1. *[Nombre del sistema B1]*

1. **Tipo de soporte:**

   a) Tipo de soporte
   b) Descripción:

2. **Características del lugar donde se resguardan los soportes:**

---

[10] En caso de que el sujeto obligado prevea cambiar el tipo de soporte que utiliza el sistema por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

[11] Precisar si el sistema se encuentra en soportes físicos, soportes electrónicos o ambos.

[12] Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

[13] Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:
a) Para soportes físicos, el sujeto obligado deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
b) Para soportes electrónicos, la descripción ofrecida por el sujeto obligado deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes, y
c) En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

[14] En caso de que dos o más sistemas se encuentren resguardados en el mismo lugar, se puede hacer una sola descripción señalando expresamente los sistemas a los que aplica.

PARTE 3. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

A1. *[Nombre del sistema A1]*

I. Transmisiones de datos personales

1. Transmisiones mediante el traslado de soportes físicos:[15]

a) Deberá señalar si el envío se realiza a través de mensajero oficial, mensajero privado o correspondencia ordinaria;[16]
b) Deberá precisar si utiliza un sobre o paquete sellado de manera que sea perceptible si fue abierto antes de su entrega;
c) Deberá manifestar si el sobre o paquete enviado es entregado en mano al destinatario, previa acreditación con identificación oficial;
d) Deberá indicar si el remitente pide al destinatario que le informe en caso de que reciba el sobre o paquete con señas de apertura;
e) Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales, y
f) Deberá señalar si el remitente registra la o las transmisiones en su bitácora así como en el Sistema Persona.

2. Transmisiones mediante el traslado físico de soportes electrónicos:

a) Deberá señalar lo previsto en el numeral 1) anterior, incisos a) al f), y
b) Deberá precisar si los archivos electrónicos que contienen datos personales son cifrados antes de su envío y proporcionar detalles técnicos del cifrado tales como el tipo de algoritmo utilizado y la longitud de la llave (o clave).[17]

3. Transmisiones mediante el traslado sobre redes electrónicas:

a) Deberá señalar la información prevista en el inciso b) del numeral 2) anterior;

---

15 **Ejemplo de medidas de seguridad para transmisiones mediante el traslado de soportes físicos:**
1. La transmisión de datos personales mediante el traslado de soportes físicos se lleva a cabo por la vía elegida de común acuerdo entre las partes: mensajero oficial, asistente secretarial, visita personal, servicio de mensajería externo, entre otras posibles. Se define un destinatario primario y otro secundario por si el mensajero no encuentra al primero.
2. El paquete con datos personales en soportes físicos viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo.
3. La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación, además de la fecha de entrega.
4. El mensajero no entrega el paquete si el destinatario no puede acreditar su identidad. En este caso, el mensajero devuelve el paquete al transmisor.
5. El transmisor verifica que el mensajero haya entregado el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente.
6. Se registran estas transmisiones en el Sistema Persona.

16 El envío por correspondencia ordinaria sólo es aceptable si los datos personales requieren de un nivel de protección básico o si los datos están disociados de sus titulares.

17 Se recomiendan los siguientes bits de longitud considerando el nivel de protección que requieren los datos personales: nivel de protección bajo, 128 bits de longitud; nivel de protección medio, 512 bits de longitud; y nivel de protección alto, 1024 bits. Estos parámetros pueden variar de acuerdo al avance o desarrollo en tecnologías de cifrado.

b) Deberá precisar si utiliza un canal de comunicación dedicado o una red privada virtual especificando detalles técnicos relativos al cifrado de dicho canal como la longitud de llave (o clave); en su caso, deberá precisar si para dicho canal utiliza una red pública (como Internet) especificando el protocolo de transmisiones protegidas utilizado;

c) Deberá manifestar si el remitente y/o el destinatario cuentan con dispositivos que faciliten la detección de intrusiones en el canal de comunicaciones.

d) Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales, y

e) Deberá señalar si el remitente registra la o las transmisiones en su bitácora así como en el Sistema Persona.

II. Resguardo de sistemas de datos personales con soportes físicos

1. *Señalar las medidas de seguridad que ha implementado el sujeto obligado para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.*[18]
2. *Señalar en un listado las personas que tienen acceso a los soportes físicos del sistema.*[19]

III. Bitácoras para accesos y operación cotidiana

1. Los datos que se registran en las bitácoras:[20]

---

[18] Por ejemplo, se espera que precise si los formatos impresos, documentos, listados o expedientes están foliados, cosidos o engargolados, si los muebles o la estantería donde residen cuentan con cerradura, si existen mecanismos para regular la temperatura y la humedad, si existen sistemas de detección y/o supresión de incendios, si cuenta con mecanismos para regular y mantener el suministro continuo de energía eléctrica, entre otras posibles medidas.

[19] En caso de ser muchas personas, se sugiere agregar el listado como Anexo al Documento de seguridad.

[20] **Ejemplo de medidas de seguridad aplicables a bitácoras para sistemas en soportes físicos:**
El Responsable del sistema procura un estricto control y registro de:
1. Las autorizaciones emitidas para facultar el acceso a un servidor público a fin de que éste, en el ejercicio de sus funciones, pueda interactuar con uno o más de los sistemas a su cargo.
2. La asignación, actualización y reemplazo de las llaves que entrega a los autorizados para que éstos puedan abrir el mecanismo de apertura de la puerta en la zona de acceso restringido.
3. Las acciones que los autorizados llevan a cabo en el área de resguardo. Para ello, designa a un Encargado quien anota lo siguiente: Quién solicita el acceso, cuándo se lleva a cabo (fecha y hora de entrada y salida), la razón que lo motiva y número del expediente utilizado.
4. El préstamo de expedientes es asistido por un sistema de cómputo que utiliza códigos de barras en los gafetes del personal autorizado y en los expedientes.
5. El sistema de préstamo de expedientes genera una bitácora electrónica que se respalda diariamente en un servidor dentro del centro de cómputo que administra el área de informática. Su integridad se garantiza copiando dicha bitácora en un CD-R diariamente.
6. El Encargado del sistema es la persona designada para analizar la bitácora cada mes mediante una herramienta adquirida para tal fin.

Ejemplo de medidas de seguridad aplicables a bitácoras para sistemas en soportes electrónicos:
1. El Responsable del sistema -en coordinación con las áreas de informática y seguridad de la información- lleva un estricto control y registro de:
   a) Las bitácoras de eventos ocurridos a nivel *sistema operativo* en los equipos (servidores, cortafuegos, almacenamiento masivo) que habilitan la operación del sistema de datos personales. Entre otras, se generan bitácoras para desempeño del servidor: intentos de acceso (exitosos y fallidos); accesos denegados a usuarios y terminales; uso de herramientas para administración del servidor, y fecha y hora de los eventos anteriores.
   b) Las bitácoras de eventos generados a nivel *software aplicativo* del sistema de datos personales. Entre otras, se generan bitácoras para mensajes de error; apertura, modificación y cierre de archivos; violaciones de seguridad detectadas por el software aplicativo, y fecha y hora de estos eventos.
   c) Las bitácoras de eventos relativos a las actividades de usuarios (capturistas, Encargados, el propio Responsable y el administrador del servidor) en su interacción con el sistema de datos personales. Entre otras, se generan bitácoras para: Archivos, servicios y recursos utilizados; intentos de acceso (exitosos y fallidos); comandos y operaciones iniciadas, y fecha y hora de dichos eventos.

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

2. *Si las bitácoras están en soporte físico o en soporte electrónico;*[21]

3. *Lugar dónde almacena las bitácoras y por cuánto tiempo;*

4. *La manera en que asegura la integridad de las bitácoras, y*

5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el sujeto obligado o si es un tercero) y cada cuándo las analiza, y
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

IV. Registro de incidentes[22]

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) La metodología aplicada;[23]

---

d) El conjunto de bitácoras permiten registrar, entre otros, los siguientes datos: Quién accede a los datos personales, desde dónde y con qué; accesos (intentos exitosos y fallidos) y salidas; propósito del acceso (sólo para modificaciones en el software aplicativo); operaciones llevadas a cabo; datos personales (registros y campos) utilizados de la base de datos, y fecha y hora de estos eventos.
e) Las bitácoras arriba mencionadas están todas en soportes electrónicos y se almacenan al menos por dos años en CD-R. Se tiene una copia en el centro de datos y otra se lleva a una bóveda bancaria subcontratada también para los respaldos.

2. La integridad de las bitácoras se garantiza copiándolas en un servidor del centro de datos el cual las graba en CD-R. Algunas se copian cada hora, otras a diario. La integridad de las copias se garantiza además con "resúmenes" creados por un algoritmo "digestor". Se cuenta con una herramienta de software que automatiza estas operaciones.
3. Las áreas de informática y seguridad de la información han designado una persona que se encarga de realizar un análisis de las bitácoras generadas. Las siguientes características aplican al caso:
   a) Se cuenta con la ayuda de una herramienta informática adquirida para tal propósito.
   b) Cada semana se llevan a cabo análisis de bitácoras pero no de todas ellas. Depende de la bitácora y de las amenazas detectadas en el entorno.
4. Se pueden realizar análisis focalizados a mayor profundidad en caso de presentarse un incidente que así lo requiera.

21 En caso de tener las bitácoras en soportes físicos, debe señalar si en el futuro planea incorporarlas a soportes electrónicos.

22 En este rubro el sujeto obligado debe describir el procedimiento de atención de incidentes que tiene implementado y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

23 **Ejemplo de procedimiento en caso de presentarse un incidente:**
a) El Encargado elabora y entrega un informe al Responsable a más tardar al día siguiente de haber ocurrido el incidente. Dicho informe precisa los soportes físicos o electrónicos afectados y, en su caso, los recuperados.
b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Dicha hoja está protegida con una contraseña de acceso. Su integridad se garantiza generando y almacenando un resumen creado por un algoritmo digestor en un servidor del centro de datos y respaldándola en un CD-R después de registrar un incidente.
c) En caso de robo o extravío de datos personales, el Responsable del sistema, al tener conocimiento del incidente, da vista al titular de la dependencia o entidad para su conocimiento y al titular del área jurídica o aquél que tenga facultades para presentar denuncias o querellas ante el Ministerio Público para que en el ámbito de sus atribuciones, determine lo conducente.

c) *Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y*
d) *Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados.*

2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

V. Acceso a las instalaciones

1. **Seguridad perimetral exterior** (las instalaciones del sujeto obligado):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?[24]

Para las personas que acceden a sus instalaciones:
a) *¿Cómo las identifica?*
b) *¿Cómo las autentifica?*
c) *¿Cómo les autoriza el acceso?*

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema?[25]

Para las personas que acceden a dichos espacios interiores:
a) *¿Cómo las identifica?*
b) *¿Cómo las autentifica?*
c) *¿Cómo les autoriza el acceso?*

VI. Actualización de la información contenida en el sistema

[Establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos].

Las medidas de seguridad previstas en los incisos VII al IX, sólo aplican para soportes electrónicos

d) A no más de 3 días naturales de haber ocurrido el incidente, el Responsable del sistema da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional.
e) En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el Responsable del sistema da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Adicionalmente, se da aviso por correo electrónico o por teléfono.

[24] Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de vídeo-vigilancia, entre otras posibles medidas.

[25] Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de vídeo-vigilancia, entre otras medidas.

VII. Perfiles de usuario y contraseñas[26]

1. Modelo de control de acceso *[alguno de los siguientes]*:

   a) *¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?*
   b) *¿Es discrecional (matriz de control de acceso)?*
   c) *¿Está basado en roles (perfiles) o grupos?*
   d) *¿Está basado en reglas?*

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

   a) *¿Cuenta con un sistema operativo de red instalado en sus equipos?*
   b) *¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?*
   c) *¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?*

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

   a) *¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?*
   b) *¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?*

4. Administración de perfiles de usuario y contraseñas:

   a) *¿Quién da de alta nuevos perfiles?*
   b) *¿Quién autoriza la creación de nuevos perfiles?*
   c) *¿Se lleva registro de la creación de nuevos perfiles?*

5. Acceso remoto al sistema de datos personales:

   a) *¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?*
   b) *¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?*
   c) *¿Cómo se evita el acceso remoto no autorizado?*

VIII. Procedimientos de respaldo y recuperación de datos

1. *Señalar si realiza respaldos completos, diferenciales o incrementales;*
2. *El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;*[27]
3. *Cómo y dónde archiva esos medios, y*
4. *Quién es el responsable de realizar estas operaciones (el sujeto obligado o un tercero).*

---

[26] En este rubro el sujeto obligado deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

[27] Es deseable que precise si para almacenar dichos medios cuenta con al menos dos lugares distintos que cumplan con las condiciones de seguridad especificadas en el articulado del Capítulo V de los Lineamientos, conforme a la fracción III del Trigésimo primero de los Lineamientos; o bien, si utiliza un espacio externo seguro para guardar de manera sistemática dichos respaldos, según la fracción VIII del Trigésimo séptimo de tales Lineamientos.

IX. Plan de contingencia

1. *Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene pero se encuentra desarrollándolo.*
2. *Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia del mismo.*
3. *Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:*
   a) *El tipo de sitio (caliente, tibio o frío);*[28]
   b) *Si el sitio es propio o sub contratado con un tercero;*
   c) *Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio, y*
   d) *Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.*

A2. *[Nombre del sistema A2]*[29]

I. Transmisiones de datos personales
II. Resguardo de sistemas de datos personales con soportes físicos
III. Bitácoras para accesos y operación cotidiana
IV. Registro de incidentes
V. Acceso a las instalaciones
VI. Actualización del sistema de datos personales
VII. Perfiles de usuario y contraseñas
VIII. Procedimientos de respaldo y recuperación de datos
IX. Plan de contingencia

B1. *[Nombre del sistema B1]*

I. Transmisiones de datos personales
II. Resguardo de sistemas de datos personales con soportes físicos
III. Bitácoras para accesos y operación cotidiana
IV. Registro de incidentes
V. Acceso a las instalaciones
VI. Actualización del sistema de datos personales
VII. Perfiles de usuario y contraseñas
VIII. Procedimientos de respaldo y recuperación de datos
IX. Plan de contingencia

---

[28] El tipo de sitio caliente, tibio o frío se refiere a la infraestructura, el equipo y el software disponibles en el sitio alterno; por lo que a mayor disponibilidad de dichos elementos resulta una menor demora para restablecer las operaciones de uno o más sistemas. Ejemplos de lo anterior son, en cuanto a **infraestructura:** aire acondicionado, cableado, suministro de energía eléctrica y enlaces de comunicaciones; en cuanto al **equipo**: servidores, almacenamiento y periféricos, y por lo que se refiere al **software:** sistemas operativos, manejadores de bases de datos y aplicaciones. Por lo tanto:

i) En un **sitio alterno caliente** se mantienen disponibles en todo momento la infraestructura, el equipo y el software; lo único que hace falta para iniciar operaciones son los datos y el personal. Este tipo de sitios alternos es el más costoso pero supone tan solo unas cuantas horas para restaurar operaciones.

ii) El **sitio alterno tibio** cuenta con infraestructura no configurada y equipos equivalentes que pueden estar disponibles en pocas horas pero no contienen software ni datos. Este tipo de sitios alternos es el punto medio en costo y tiempo para restaurar operaciones.

iii) El **sitio alterno frío** cuenta con un ambiente mínimo de infraestructura y no cuenta con el equipo. Este tipo de sitios alternos es el menos costoso pero supone demora de algunos días para restablecer operaciones.

[29] Se debe seguir el modelo del sistema A1 –incisos I al IX- para señalar las medidas de seguridad aplicables a cada uno de los sistemas que posea el sujeto obligado.

PARTE 4. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE DATOS PERSONALES

[Informar y describir el procedimiento para la cancelación de un sistema de datos personales.][30]

1. **Datos del sistema que será cancelado:**

   a) Denominación

   b) Folio del Sistema Persona

   c) Motivo de la cancelación

2. **Plazos y condiciones para el bloqueo del sistema:**[31]

   [Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad específica de cada sujeto obligado. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo]

3. **Medidas de seguridad para el bloqueo y posterior supresión del sistema:**

   [Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema]

---

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

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

La cancelación de sistemas de datos personales debe considerar lo establecido en los Lineamientos generales para la organización y conservación de archivos de las Dependencias y Entidades de la Administración Pública Federal y en concordancia con ello, el sujeto obligado debe establecer un procedimiento de cancelación en su Documento de seguridad, en términos de lo que establecen el Trigésimo tercero y el Trigésimo cuarto de los Lineamientos de protección de datos, el cual deberá hacerse del conocimiento del titular de los datos.

En el Primero de los Lineamientos de archivos se establecen criterios de organización y conservación de la documentación de las dependencias y entidades de la APF con el objeto de conservar íntegros y disponibles los documentos para permitir y facilitar el acceso a la información que contengan. Dichos Lineamientos de archivo establecen además que se debe incluir la siguiente información en el Catálogo de disposición documental -un registro general y sistemático que establece los siguientes valores documentales-: (i) los plazos de conservación; (ii) la vigencia documental; (iii) la clasificación de reserva o confidencialidad, y (iv) el destino final de los documentos.

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

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

[31] Es el periodo por el que se conservará para efectos de responsabilidades, tomando en cuenta el plazo de su prescripción conforme la normatividad aplicable.

4. Procedimiento para la supresión del sistema

[Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo]

5. Mecanismos para la supresión del sistema.

[Describir las técnicas para la eliminación física del sistema] [32]

[32] Cuando el sistema almacene datos personales en **soportes físicos**, se recomienda incluir en el procedimiento de cancelación alguna de las técnicas conocidas para la destrucción de este tipo de soportes, como es la trituración o la incineración de documentos. Ahora bien, en caso de que almacene datos personales en **soportes electrónicos**, las características de la información requieren que el sujeto obligado "purgue" los archivos contenidos en los medios de almacenamiento -o bien, que destruya tales medios- toda vez que es insuficiente borrar los archivos o "darle formato" al medio de almacenamiento.

Con el fin de garantizar la efectiva destrucción de los datos contenidos en soportes electrónicos, se recomienda que el procedimiento de cancelación incluya al menos una de las siguientes técnicas:

a) Sobrescribir con un solo valor (unos o ceros) el 100% de la superficie de los medios de almacenamiento no volátil en los que residen los datos del sistema cancelado. Esta técnica es efectiva para discos duros.
b) Desmagnetización de medios magnéticos mediante una herramienta especializada conocida como desmagnetizador o "degausser". Esta técnica es efectiva para discos duros y cintas magnéticas.
c) Destrucción física de los medios de almacenamiento. La Guía para la Sanitización de Medios ("*Guidelines for Media Sanitization*") que fue publicada por el Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology)* de los Estados Unidos de América, recomienda fundir, desintegrar, desmoronar, pulverizar o incinerar los soportes electrónicos.
d) Cualquier otra técnica utilizada por el sujeto obligado que tenga por objeto la destrucción de soportes electrónicos.

PARTE 5. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

Responsable del desarrollo:

[Señalar nombre, puesto, teléfono y correo electrónico del servidor público que elaboró el documento de seguridad]

Revisó:

[Señalar nombre, puesto, teléfono y correo electrónico del servidor público que revisó el documento de seguridad]

Autorizó:

[Señalar nombre, puesto, teléfono y correo electrónico del servidor público que autorizó el documento de seguridad]

Fecha:

[Incluir la fecha de liberación del documento]

PARTE 6. ANEXOS TÉCNICOS

[En este apartado se deberán enumerar los anexos e identificarlos con su denominación.
Los anexos deberán adjuntarse en el orden en el que se enlisten en este apartado y en la parte superior de cada uno deberá estar indicado el número que le corresponde y su denominación para facilitar su identificación]