**Fondo de Garantía y Fomento para la Agricultura, Ganadería y Avicultura**

**DOCUMENTO DE SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES**

**Contenido**

|  |  |  |
| --- | --- | --- |
| Tema | Página |  |
| Introducción  Marco Jurídico | 2 |  |
| 1. Derechos de los titulares de los datos | 7 |  |
| 1. Inventario de sistemas de tratamiento | 10 |  |
| 3. Funciones y obligaciones de las personas que tratan datos personales. | 12 |  |
| 4. Análisis de riesgos | 13 |  |
| 5. Análisis de brechas |  |  |
| 6. Plan de trabajo |  |
| 7. Mecanismos de monitoreo y revisión de las medidas de seguridad implementadas |  |
| 8. Programa general de capacitación |  |
| 9. Anexos |  |

**Introducción**

Derivado de la puesta en marcha de la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, la gestión de la seguridad en la información en instituciones públicas cada día es más relevante en el país, el cambio de cultura en los ciudadanos se va permeando poco a poco en diferentes esferas de la sociedad, debido a que el uso de los datos personales con las nuevas tecnologías es cada vez mayor y con una velocidad inimaginable.

Regular las actividades relativas al control de datos personales en cada una de las organizaciones, es una labor que ha venido realizando el Instituto Nacional de Transparencia y Acceso a la Información Pública y protección de Datos (INAI), desde hace más de una década.

En esta parte es muy importante la participación de todos y cada uno de los servidores públicos, por lo que en la medida que se encuentren debidamente informados, se podrá establecer una debida gestión de tratamiento, buscando la implementación de mejores medidas de control a la confidencialidad, integridad y disponibilidad de los datos personales.

La idea principal es que de alguna manera las dependencias y entidades de la Administración Pública Federal establezcan y en su caso mejoren las medidas de seguridad en los procesos, herramientas informáticas o sistemas diseñados y administrados por cada una de ellas en el nivel que le corresponda.

Las vulneraciones a la seguridad de la información, puede ocurrir en cualquier fase del tratamiento de los datos personales y podría afectar los derechos patrimoniales o morales de los titulares, debido a la pérdida o destrucción no autorizada, robo, extravío, copia no autorizada, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de los datos personales.

En el presente documento se presenta el inventario de sistemas que cuentan con datos personales cédulas descriptivas de los mismos, medidas de protección establecidas por la Entidad, para el debido tratamiento de la información que contenga datos personales en cada una de las Unidades Administrativas, programas de capacitación y análisis de brechas entre otros.

**Marco jurídico**

Artículo 16 Constitucional:

“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 cual establecerá los supuestos de excepción 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”.

De conformidad con lo establecido en el artículo 35 en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los responsables de tratar datos personales deben elaborar un documento de seguridad que contenga, al menos, lo siguiente:

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

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

**III.** El análisis de riesgos;

**IV.** El análisis de brecha;

**V.** El plan de trabajo;

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

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

Asimismo, dicho ordenamiento legal en su artículo 36, señala que el responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:

**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, y

**IV.** Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Por otra parte, en el artículo de la 84, de la Ley General de Protección de Datos Personales, el Comité de Transparencia tendrá las siguientes funciones:

**I.** Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;

**II.** Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;

**III.** Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;

**IV.** Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;

**V.** Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;

**VI.** Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto y los organismos garantes, según corresponda;

**VII.** Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y

**VIII.** Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.

Derivado de lo anterior, y para una mejor referencia, se indican las definiciones y conceptos que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO):

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

**Datos Personales**. - Cualquier información concerniente a una persona física identificada o identificable.

**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;

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

**Titular. -** La persona física a quien corresponden los datos personales.

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

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

**Responsable:** Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales.

Así mismo, se observan los siguientes principios en el tratamiento de datos personales:

**Principio de Licitud.** - El tratamiento de datos personales por parte de FIRA, debe sujetarse a las facultades o atribuciones que la normativa aplicable le confiera.

**Principio de Finalidad**. - Todo tratamiento de datos personales que se efectúe deberá ser justificado por finalidades concretas, licitas, explicitas, y legitimas relacionadas con las atribuciones que la normativa aplicable les confiera.

**Principio de Lealtad**. - No se deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

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

**Principio de Calidad**. - Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales, sin alterar la veracidad de los mismos.

**Principio de Proporcionalidad**. - Se deben tratar solo aquellos datos personales que resulten estrictamente necesarios, adecuados y relevantes en relación con las finalidades para los cuales se obtuvieron.

**Principio de Información.** - Se deberá comunicar a los titulares de los datos personales, la información que se recaba de ellos, las características principales del tratamiento y con qué fines se recaban los datos. (Esto se llevará a cabo mediante el Aviso de privacidad).

**Principio de Responsabilidad (Principio de rendición de cuentas). -** Establecer mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones que determine la normativa aplicable tanto en el ámbito nacional, como en el internacional.

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

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

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

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

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

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

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

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

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

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

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

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

**DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES**

1. Ser informado a través del aviso de privacidad, respecto de la existencia y características principales del tratamiento al que serán sometidos sus datos personales.

2. Que sean bloqueados y posteriormente suprimidos sus datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad.

3. Ser previamente informado, para el caso de que exista alguna transmisión, de quienes serán los destinatarios de sus datos personales y que no se hubiera señalado en el aviso de privacidad correspondiente.

4. Realizar el ejercicio de los derechos ARCO (acceso, rectificación, cancelación y oposición).

**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 INAI:

* **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

### 

### **Controles y mecanismos de seguridad para las transferencias**

Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes, exceptuando las realizadas entre responsables en cumplimiento de una disposición legal o en el ejercicio de sus atribuciones, así mismo en el ámbito internacional cuando se encuentren previstas en una ley o tratado suscrito y ratificado por México, o sea solicitada por una autoridad u organismo internacional competente.

**Transferencias mediante el traslado de soportes físicos**

La seguridad física consiste en la aplicación de barreras físicas, y procedimientos de control como medidas de prevención y contra medidas ante amenazas a los recursos y la información confidencial, se refiere a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas informáticos, así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

**Transferencias mediante el 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.

Al realizar transferencias físicas de soportes electrónicos se deberá considerar los dispuesto en los ordenamientos aplicables, como lo son: Los oficios de comisión para el personal autorizado y asegurar que la entrega sea a los titulares de la información o a personal autorizado para recibirla, los medios para garantizar la confidencialidad de la información, utilizar las leyendas de clasificación, registro en bitácoras de transferencia, cifrar la información, utilizar contraseñas etc…

**Transferencias mediante el 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.

# **Técnicas de Supresión y Borrado Seguro de Datos Personales**

(Ciberseguridad)

Los medios eficaces que evitan completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento son: la desmagnetización, la destrucción y la sobreescritura en la totalidad del área de almacenamiento de la información.

**Desmagnetización**

La desmagnetización consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo.

Este método es válido para la destrucción de datos de los dispositivos magnéticos, como por ejemplo, los discos duros, disquetes, cintas magnéticas de backup, etc. Cada dispositivo, según su tamaño, forma y el tipo de soporte magnético de que se trate, necesita de una potencia específica para asegurar la completa polarización de todas las partículas.

**Destrucción física**

El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos que almacena. Existen diferentes tipos de técnicas y procedimientos para la destrucción de medios de almacenamiento: desintegración, pulverización, fusión e incineración: son métodos diseñados para destruir por completo los medios de almacenamiento. Estos métodos suelen llevarse a cabo en una destructora de metal o en una planta de incineración autorizada, con las capacidades específicas para realizar estas actividades de manera eficaz, segura y sin peligro.

Trituración: las trituradoras de papel se pueden utilizar para destruir los medios de almacenamiento flexibles. El tamaño del fragmento de la basura debe ser lo suficientemente pequeño para que haya una seguridad razonable en proporción a la confidencialidad de los datos que no pueden ser reconstruidos.

Los medios ópticos de almacenamiento (CD, DVD, magneto-ópticos) deben ser destruidos por pulverización, trituración de corte transversal o incineración. Cuando el material se desintegra o desmenuza, todos los residuos se reducen a cuadrados de cinco milímetros (5mm) de lado. Como todo proceso de destrucción física, su correcta realización implica la imposibilidad de recuperación posterior por ningún medio conocido. En el caso de los discos duros se deberá asegurar que los platos internos del disco han sido destruidos eficazmente, no sólo la cubierta externa.

**Sobre-escritura**

La sobre-escritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento. La sobre-escritura se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados, por lo que no se puede utilizar en aquellos que están dañados ni en los que no son regrabables, como los CD y DVD. 1.

1. Guía Práctica para elaborar un documento de seguridad. Instituto de la Transparencia, información pública y protección de datos personales del estado de Jalisco.

Por otra parte, entre los diferentes procedimientos y políticas que permiten establecer de mejor manera las medidas de seguridad de la información, se tiene establecida la siguiente normativa interna:

* Procedimiento operativo en materia de protección de datos personales.
* Medidas de seguridad para el control de acceso y uso de las instalaciones.
* Controles de seguridad de la información en FIRA
* Procedimiento operativo de seguridad informática
* Procesos en las materias de TIC y de seguridad de la información.

1. **Inventario de Sistemas de Tratamiento.**

Unidad Administrativa que custodia los sistemas:Subdirección de Infraestructura Informática

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Nombre del Sistema** | **Denominación Genérica** | | **Unidad Administrativa responsable** | **UA responsable del desarrollo** |
|  | **Categoría** | **Subcategoría** |
|  |  |  |  |  |  |
| 1 | **SISTEMA DE COBRANZA A EX EMPLEADOS** | SERVICIOS ADMINISTRATIVOS | GESTIÓN DE PERSONAL | Subdirección de Cartera | Subdirección de Sistemas Informáticos Institucionales |
| 2 | **MODULO SIPROCURA** | SERVICIOS FINANCIEROS | CRÉDITOS | Subdirección de Cobranza y Seguimiento a Garantías Pagadas | Subdirector de Sistemas Informáticos para Procesos de Negocio |
| 3 | **MODULO SIRRECUPERA** | SERVICIOS FINANCIEROS | BENEFICIARIOS | Subdirección de Cobranza y Seguimiento a Garantías Pagadas | Subdirector de Sistemas Informáticos para Procesos de Negocio |
| 4 | **SUSTRAE** | SERVICIOS FINANCIEROS | BENEFICIARIOS | Subdirección de Cobranza y Seguimiento a Garantías Pagadas | Subdirección de Sistemas Informáticos para la administración de Riesgos |
| 5 | **DESARROLLO DE DATOS MAESTROS SISTEMA INTEGRA- CD** | SERVICIOS ADMINISTRATIVOS | CLIENTES | Subdirección de Contabilidad | Subdirección de Sistemas Informáticos Institucionales |
| 6 | **DESARROLLO DE DATOS MAESTROS SISTEMA INTEGRA- E** | SERVICIOS ADMINISTRATIVOS | GESTIÓN DE PERSONAL | Subdirección de Contabilidad | Subdirección de Sistemas Informáticos Institucionales |
| 7 | **DESARROLLO DE DATOS MAESTROS SISTEMA INTEGRA- PA** | SERVICIOS ADMINISTRATIVOS | PROVEEDORES | Subdirección de Contabilidad | Subdirección de Sistemas Informáticos Institucionales |
| 8 | **SISTEMA DE ADMINISTRACIÓN DE APOYOS** | SERVICIOS FINANCIEROS | BENEFICIARIOS | Subdirección de Operaciones | Subdirección de Sistemas Informáticos Institucionales |
| 9 | **CAPITAL HUMANO PENSIONADOS** | SERVICIOS ADMINISTRATIVOS | GESTIÓN DE PERSONAL | Subdirección de Recursos Humanos | Subdirección de Sistemas Informáticos Institucionales |
| 10 | **EBIS** | SERVICIOS ADMINISTRATIVOS | GESTIÓN DE PERSONAL | Subdirección de Recursos Humanos | Subdirección de Sistemas Informáticos Institucionales |
| 11 | **MÓDULO DE GASTOS MÉDICOS** | SERVICIOS ADMINISTRATIVOS | GESTIÓN DE PERSONAL | Subdirección de Recursos Humanos | Subdirección de Sistemas Informáticos Institucionales |
| 12 | **MÓDULO DE SEGUROS** | SERVICIOS ADMINISTRATIVOS | NOMINAS | Subdirección de Recursos Humanos | Subdirección de Sistemas Informáticos Institucionales |
| 13 | **SISTEMA DE CAPITAL HUMANO** | SERVICIOS ADMINISTRATIVOS | GESTIÓN DE PERSONAL | Subdirección de Recursos Humanos | Subdirección de Sistemas Informáticos Institucionales |
| 14 | **SISTEMA DE EXPEDIENTES DIGITALIZADOS DEL PERSONAL ACTIVO, PENSIONADO Y EXEMPLEADOS DE LA INSTITUCIÓN** | REGISTROS-IDENTIFICACIÓN | DOCUMENTACIÓN PERSONAL | Subdirección de Recursos Humanos | Subdirección de Sistemas Informáticos Institucionales |
| 15 | **SISTEMA DE INGRESOS POR SALARIOS** | SERVICIOS ADMINISTRATIVOS | NOMINAS | Subdirección de Recursos Humanos | Subdirección de Sistemas Informáticos Institucionales |
| 16 | **SISTEMA DE RECURSOS HUMANOS Y PRÉSTAMOS** | SERVICIOS ADMINISTRATIVOS | GESTIÓN DE PERSONAL | Subdirección de Recursos Humanos | Subdirección de Sistemas Informáticos Institucionales |
| 17 | **SISTEMA ÚNICO DE AUTODETERMINACIÓN SUA** | SERVICIOS ADMINISTRATIVOS | NOMINAS | Subdirección de Recursos Humanos | Subdirección de Sistemas Informáticos Institucionales |
| 18 | **TRANSACCIONES PA20, PA30 Y PA40 EN EL SISTEMA INTEGRA** | SERVICIOS ADMINISTRATIVOS | GESTIÓN DE PERSONAL | Subdirección de Recursos Humanos | Subdirección de Sistemas Informáticos Institucionales |
| 19 | **MÓDULO DE MATERIALES EN EL SISTEMA INTEGRA** | SERVICIOS ADMINISTRATIVOS | PROVEEDORES | Subdirección de Adquisiciones | Subdirección de Sistemas Informáticos Institucionales |
| 20 | **IDENTIFICACIÓN DE ACREDITADOS POTENCIALES CON MECANISMOS PARAMÉTRICOS** | SERVICIOS FINANCIEROS | BENEFICIARIOS |  | Subdirección de Sistemas Informáticos Institucionales |
| 21 | **SAS-SIIOF** | SERVICIOS FINANCIEROS | CRÉDITOS | Subdireccion de Cartera | Subdirector de Sistemas Informáticos para Procesos de Negocio |
| 22 | **EXPEDIENTE DIGITAL DE PROVEEDORES** | SERVICIOS ADMINISTRATIVOS | PROVEEDORES | Subdirección de Adquisiciones | Subdirección de Sistemas Informáticos Institucionales |

1. **Funciones y obligaciones de las personas que tratan datos personales**

**Funciones:**

* Realizar la captura adecuada de la información en los sistemas que tiene acceso el servidor público, en la cual se incluyan datos personales, observando principios en el tratamiento de datos personales.
* Mantener almacenados los soportes documentales que contengan datos de carácter personal, en lugares a los que no tenga acceso el personal no autorizado.
* Utilizar para las labores que tiene asignadas, los sistemas de información, recursos, y en su caso la información física a la que el servidor público accede.
* Quienes tengan acceso a información con datos personales sensibles, deben limitarse al acceso que el desarrollo de sus funciones asignadas lo requiera.

**Obligaciones:**

* Custodiar y cuidar la documentación e información que, por razón de sus actividades, cargo o comisión, tengan bajo su responsabilidad, e impedir o evitar su uso, divulgación, sustracción, destrucción, ocultamiento o inutilización indebidos.
* Proteger los datos personales que esté tratando y custodiarlos para que personal no autorizado no tenga acceso a ellos.
* Guardar secreto y confidencialidad de la información tratada.
* Facilitar el derecho de acceso, rectificación y cancelación a los titulares de los datos (ejercicio de derechos ARCO) de conformidad con lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
* Observar las medidas de seguridad establecidas en la institución y que se encuentren debidamente documentadas ya sea en los procedimientos operativos, avisos administrativos, políticas internas entre otros.
* Tener identificada la información de datos personales que trata tanto de forma física, como en archivos electrónicos.
* Dar aviso al jefe inmediato en caso de detectar alguna vulnerabilidad a la información tratada. (ver documento “Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales”).

**TRATAMIENTO MANUAL DE DATOS PERSONALES**

En lo que se refiere a los documentos con datos personales que se tengan en archivos físicos, quienes se encuentren a su cargo deberán custodiarlos e impedir el acceso de personas no autorizadas.

Siempre que se proceda al traslado físico de la documentación contenida bajo el resguardo de alguno de los empleados de la institución, deberán adoptarse las medidas que impidan el acceso indebido, manipulación, sustracción o pérdida de la información objeto del traslado durante el transporte de la misma.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. **Análisis de riesgos.**

No se considera esta información para su publicación

1. **Análisis de brechas.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Análisis de Brecha***  ***(Medidas de seguridad existentes VS medidas de seguridad faltantes)*** | | | | |
| *Código* | Pregunta o Control | ¿Existente? | | |
| Sí | No | Observaciones |
| A. | Medidas de seguridad basadas en la cultura del personal | | | |
| A.1. | *¿Pones atención en no dejar a la vista información*  *personal y llevas registro de su manejo?* |  |  |  |
| *A.1.1.* | Política de escritorio limpio |  |  |  |
| *A.1.2.* | Hábitos de cierre y resguardo |  |  |  |
| *A.1.3.* | Impresoras, escáneres, copiadoras y buzones limpios |  |  |  |
| *A.1.4.* | Gestión de bitácoras, usuarios y acceso |  |  |  |
| A.2. | *¿Tienes mecanismos para eliminar de manera segura la*  *información?* |  |  |  |
| *A.2.1.* | Destrucción segura de documentos |  |  |  |
| *A.2.2.* | Eliminación segura de información en equipo de  cómputo y medios de almacenamiento electrónico |  |  |  |
| *A.2.3.* | Fijar periodos de retención y destrucción de información |  |  |  |
| *A.2.4.* | Tomar precauciones con los procedimientos de re-  utilización |  |  |  |
| A.3. | *¿Has establecido y documentado los compromisos*  *respecto a la protección de datos?* |  |  |  |
| *A.3.1.* | Informar al personal sobre sus deberes mínimos de  seguridad y protección de datos |  |  |  |
| *A.3.2.* | Fomentar la cultura de la seguridad de la información |  |  |  |
| *A.3.3.* | Difundir noticias en temas de seguridad |  |  |  |
| *A.3.4.* | Prevenir al personal sobre la *Ingeniería Social* |  |  |  |
| *A.3.5.* | Asegurar la protección de datos personales en  subcontrataciones |  |  |  |
| A.4. | *¿Tienes procedimientos para actuar ante vulneraciones a*  *la seguridad de los datos personales?* |  |  |  |
| *A.4.1.* | Tener un procedimiento de notificación |  |  |  |
| *A.4.2.* | Realizar revisiones y auditorías |  |  |  |
| A.5. | *¿Realizas respaldos periódicos de los datos personales?* |  |  |  |
|  |  |  |  |  |
| B. | Medidas de seguridad en el entorno de trabajo físico | | | |
| B.1. | *¿Tienes medidas de seguridad para acceder al entorno de*  *trabajo físico?* |  |  |  |
| *B.1.1.* | Alerta del entorno de trabajo |  |  |  |
| *B.1.2.* | Mantener registros del personal con acceso al entorno  de trabajo |  |  |  |
| B.2. | *¿Tienes medidas de seguridad para evitar el robo?* |  |  |  |
| *B.2.1.* | Cerraduras y candados |  |  |  |
| *B.2.2.* | Elementos disuasorios |  |  |  |
| *B.2.3.* | Minimizar el riesgo oportunista |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Análisis de Brecha***  ***(Medidas de seguridad existentes VS medidas de seguridad faltantes)*** | | | | |
| *Código* | Pregunta o Control | ¿Existente? | | |
| Sí | No | Observaciones |
| B.3. | *¿Cuidas el movimiento de información en entornos de*  *trabajo físicos?* |  |  |  |
| *B.3.1.* | Aprobación de salida de documentos, equipo de  cómputo y/o medios de almacenamiento electrónico |  |  |  |
| *B.3.2.* | Mantener en movimiento sólo copias de la información,  no el elemento original |  |  |  |
| *B.3.3.* | Usar mensajería certificada |  |  |  |
| C. | Medidas de seguridad en el entorno de trabajo digital | | | |
| C.1. | *¿Realizas actualizaciones al equipo de cómputo?* |  |  |  |
| C.2. | *¿Revisas periódicamente el software instalado en el*  *equipo de cómputo?* |  |  |  |
| C.3. | *¿Tienes medidas de seguridad para acceder al entorno de*  *trabajo electrónico?* |  |  |  |
| *C.3.1.* | Uso de contraseñas y/o cifrado |  |  |  |
| *C.3.2.* | Uso de contraseñas solidas |  |  |  |
| *C.3.3.* | Bloqueo y cierre de sesiones |  |  |  |
| *C.3.4.* | Administrar usuarios y accesos |  |  |  |
| C.4. | *¿Revisas la configuración de seguridad del equipo de*  *cómputo?* |  |  |  |
| C.5. | *¿Tienes medidas de seguridad para navegar en entornos*  *digitales?* |  |  |  |
| *C.5.1.* | Instalar herramientas antimalware y de filtrado de  tráfico |  |  |  |
| *C.5.2.* | Reglas de navegación segura |  |  |  |
| *C.5.3.* | Reglas para la divulgación de información |  |  |  |
| *C.5.4.* | Uso de conexiones seguras |  |  |  |
| C.6. | *¿Cuidas el movimiento de información en entornos de*  *trabajo digitales?* |  |  |  |
| *C.6.1.* | Validación del destinatario de una comunicación |  |  |  |
| C.6.2. | Seguridad de la información enviada y recibida |  |  |  |

1. **Mecanismos de monitoreo y revisión de las medidas de seguridad implementadas.**

Los mecanismos para el monitoreo y revisión de las medidas de seguridad de la información y los sistemas, se encuentran establecidos en diversos documentos de carácter externo e interno, mismos que a continuación se indican:

1. **Procedimientos o guías para diseñar, desarrollar, probar y poner en producción un Sistema o módulo de datos personales.**

* ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias.
* Procesos en las materias de TIC y de seguridad de la información.
* Controles de seguridad de la información en FIRA

1. **Procedimientos o guías para generar, asignar, distribuir, modificar, almacenar y dar de baja usuarios y claves de acceso para la operación de los Sistemas de datos personales.**

* Manual Administrativo de aplicación general en materia de Tecnologías de la Información y Telecomunicaciones “MAAGTIC”.
* Procedimiento de administración de cambios.

1. **Relación de las bitácoras del sistema o módulo de datos personales, que detallen las acciones llevadas a cabo en el mismo.**

* Bitácora de modificaciones del sistema.

1. **Procedimiento o guía para la cancelación de un Sistema o módulo de datos personales.**

* Manual Administrativo de aplicación general en materia de Tecnologías de la Información y Telecomunicaciones “MAAGTIC”.

1. **Plan de trabajo.**

No se considera esta información para su publicación.

1. **Programa general de capacitación.**

Como parte del programa general de capacitación, es indispensable que todo el personal de la institución tenga una capacitación mínima en materia de protección de datos personales, misma que se considera establecer de forma anual y con el apoyo del personal del Departamento de Evaluación y Capacitación de la Entidad.

A continuación, se menciona de manera enunciativa más no limitativa, el personal de la institución que por el rol que desempeñan y por tener mayor contacto con el tema del tratamiento de datos personales, se considera incluir en la capacitación:

* + Personal de la Subdirección de Recursos Humanos.
  + Personal que maneja o trabaja en los sistemas que contienen datos personales y que se enuncian en el presente documento.
  + Personal de las áreas de jurídico, contabilidad y adquisiciones.
  + Personal de las áreas de sistemas e informática.
  + Personal que trate datos personales.
  + Demás personal de la institución. (Para conocimiento de sus derechos y obligaciones)
  + Personal de recién ingreso.

**Temario de la capacitación.**

Los puntos que se consideran en la capacitación son los siguientes:

1. Normativa relacionada con la Protección de Datos Personales.

2. Derechos de los Titulares de Datos Personales.

3. Ejercicio de los Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

4. Transferencias de Datos.

5. Infracciones, Sanciones y Delitos.

**Periodos de la capacitación:**

Se considera realizar capacitaciones anuales, en las fechas que se determinen con el Departamento de Evaluación y Capacitación de la Entidad y de acuerdo al programa anual de capacitación emitido por el INAI.

1. **Anexos**

Sistema de Gestión de Seguridad de Datos Personales

A) Establecer medidas especiales en función de ciertos factores riesgo inherente de los datos, su sensibilidad, el desarrollo tecnológico, las transferencias que se hagan y las vulneraciones a la seguridad ya ocurridas;

Otras

B) Implementar un Sistema de Gestión de la seguridad de los datos personales;

C) Elaborar un Documento de Seguridad que describa los elementos indispensables que permitirán asegurar un cuidado adecuado de los datos personales.

**Bibliografía**

* Ley General de Protección de datos Personales en Posesión de Sujetos Obligados.
* Procedimiento operativo en materia de protección de datos personales.
* Medidas de seguridad para el control de acceso y uso de las instalaciones.
* Controles de seguridad de la información en FIRA
* Procedimiento operativo de seguridad informática
* Procesos en las materias de TIC y de seguridad de la información.

**Guía para el borrado seguro de Datos personales**

Guía Práctica para elaborar un documento de seguridad. Instituto de la Transparencia, información pública y protección de datos personales del estado de Jalisco.

Ciberseguridad, I. N. (s.f.). *Guía sobre borrado seguro de la información*. Recuperado el 13 de 07 de 2018, de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia\_ciberseguridad\_borrado\_seguro\_metad.pdf

Instituto Nacional de Transparencia, A. a. (Junio de 2018). *Instituto Nacional de Transparencia, Acceso a la Información.* Recuperado el 03 de 08 de 18, de Recomendaciones para el manejo de incidentes de seguridad de datos personales: http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones\_Manejo\_IS\_DP.pdf

ProtektNet. (s.f.). Recuperado el 02 de 08 de 2018, de https://protektnet.com/servicios/cumplimiento-normativo/analisis-de-brecha-de-seguridad-de-la-informacion/

Pública, I. F. (19 de 07 de 2009). *Guía para la elaboración de un Documento de seguridad v1.4* . Recuperado el 13 de 07 de 2018, de https://www.ichitaip.org/infoweb/archivos/reader/pdp/Guia\_elaboracion\_Documento\_seguridad.pdf

Pública, I. F. (Marzo de 2014). *Son tus datos.* Recuperado el 13 de Julio de 2018, de https://sontusdatos.org/wp-content/uploads/2013/04/ifai-metodologia-de-Riesgo-BAA\_2014.pdf