PODER JUDICIAL
DEL ESTADO DE CHIAPAS

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES 2022

Contenido

GLOSARIO DE TÉRMINOS COMUNES 2

INTRODUCCIÓN 6

EL INVENTARIO DE DATOS PERSONALES (anexo 05) 8

MEDIDAS DE SEGURIDAD DE DATOS PERSONALES (anexo 06) 11

ANALISIS DE RIESGO DE LOS DATOS PERSONALES (anexo 07) 14

TIPO DE LOS DATOS PERSONALES. 14

NIVELES DE RIESGO 16

EJEMPLO DE NIVEL DE RIESGO DEL GRUPO DE DATOS IDENTIFICATIVOS: 17

EJEMPLO DE NIVEL DE RIESGO DEL GRUPO DATOS PERSONALES SENSIBLES ESPECIALMENTE PROTEGIDOS: 18

PROPÓSITO DEL ANÁLISIS DE RIESGO 18

EL ANÁLISIS DE BRECHA, MEDIDAS DE SEGURIDAD FALTANTES (anexo 08) 19

PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE LAS MEDIDAS DE SEGURIDAD FALTANTES (anexo 09) 20

VULNERACIÓN DE DATOS PERSONALES 22

PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD 22

INCIDENTES DE SEGURIDAD QUE AFECTAN DATOS PERSONALES 24

BITÁCORA DE INCIDENTES (anexo 10) 27

NOTIFICACIÓN DE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES 29

BENEFICIOS DE LA NOTIFICACIÓN DE VULNERACIONES 29

PROCESO DE NOTIFICACIÓN DE VULNERACIONES 29

LOS MECANISMOS DE MONITOREO Y REVISIONES DE LAS MEDIDAS DE SEGURIDAD (sujeto al plan de trabajo de la Contraloría Interna) 32

LAS AUDITORÍAS 32

LAS REVISIONES ADMINISTRATIVAS 32

PROGRAMA GENERAL DE CAPACITACIÓN (anexo 11). 33

DE LAS MEDIDAS DE APREMIO 34

DE LAS RESPONSABILIDADES ADMINISTRATIVAS Y SUS SANCIONES 35

LAS SANCIONES DE CARÁCTER ECONÓMICO NO PODRÁN SER CUBIERTAS CON RECURSOS PÚBLICOS. 36

BIBLIOGRAFÍA CONSULTADA 38

GLOSARIO DE TÉRMINOS COMUNES

Activo: Es todo componente al que la Institución le otorga un valor para el tratamiento de los datos personales, tales como el personal, hardware, software, archivos, documentos en papel y cualquier otro recurso involucrado.

Aceptar El riesgo: decisión informada para coexistir con un nivel de riesgo.

Amenaza: Circunstancia o evento con la capacidad de causar daño a la Institución.

Archivista (enlace): Persona designada por el responsable de la instancia (funcionario judicial o administrativo), para realizar la función de garantizar la seguridad de los datos personales que se procesan.

Auditoría: Proceso sistemático y documentado para obtener evidencias y evaluarlas de manera objetiva para determinar el grado de cumplimiento de los criterios preestablecidos para la misma.

Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, a partir del momento en el cual se recaban sus datos personales, con el objetivo de informarle los propósitos del tratamiento de los mismos.

Bases de datos: El conjunto ordenado de datos personales referentes a una persona física identificada o identificable.

Consejo: Consejo de la Judicatura del Estado de Chiapas.

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública, 62 y 63 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

Comunicar el riesgo: Compartir o intercambiar información entre la Consejo de la Judicatura, vigilantes y demás involucrados acerca del riesgo.

Compartir el riesgo: Proceso donde se involucra a terceros para mitigar la pérdida generada por un riesgo en particular, sin que el dueño del activo afectado reduzca su responsabilidad.

Confidencialidad: Es aquella garantía de que la información obtenida no puede estar a disposición de terceros o ser revelada a personas, entidades o procesos no autorizados.

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.

Datos biométricos: Se encuentran dentro de la categoría de datos sensibles, sin embargo, estos se refieren a las características físicas, fisiológicas, biológicas, firma autógrafa y ADN, cuyas descripciones refieren al comportamiento o rasgos de las personas, como pueden ser de manera enunciativa mas no limitativa, estos son la imagen del iris, rasgos faciales, patrón de la voz y huella digital.

Derechos ARCO: Garantía individual establecida en el artículo 16 de la Constitución Política Mexicana, cuyos derechos son; acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Disponibilidad: Propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados.

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

Encargado: La persona física o moral, pública o privada, ajena a la Institución del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia

de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Enlace (archivista): Persona designada por el responsable de cada área, para realizar la función de garantizar la seguridad de los datos personales que se procesan.

Evaluación de impacto en la protección de datos personales: Evaluación mediante se pretenda poner en operación o modificar políticas públicas, servicios, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, deberá presentarse ante el Instituto para la valoración de los impactos reales, es decir, si las operaciones de tratamiento de datos suponen un riesgo o el riesgo a fin de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

Evitar el riesgo: Acción para soslayarse de una situación de riesgo o decisión para no involucrarse en él.

Identificar el riesgo: Proceso de localización, registro y descripción de los elementos del riesgo.

Incidente: Escenario donde se pone en riesgo los sistemas y servicios lo que puede provocar la pérdida, modificación, destrucción o acceso no autorizado a los datos personales.

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Instancias: Áreas administrativas y Jurisdiccionales del Consejo de la Judicatura prevista en el Código de Organización, el Reglamento Interior, estatutos orgánicos o instrumentos equivalentes, que cuenten o puedan llegar a contar, que den tratamiento, y que sean responsables o encargadas de los datos personales.

ITAIPCH: Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas.

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

Ley Estatal: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

Ley de archivos: Ley General de Archivos.

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

Lineamientos Estatales: Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas**.**

Lineamientos para la evaluación de impacto: Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.

Lineamientos para la portabilidad: Acuerdo mediante el cual se aprueban los lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de 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.

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

Responsable (Poder Judicial): Funcionario delegado por el presidente del Tribunal Superior de Justicia y del Consejo de la Judicatura como titular de la instancia responsable del tratamiento de los datos personales del área a su cargo.

Retención del riesgo: Aceptación de la pérdida generada por un riesgo en particular. Esta acción implica monitoreo constante del riesgo retenido.

Revisión: Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo, de los contenidos establecidos en este Programa.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

Riesgo residual: El riesgo remanente después de tratar el riesgo.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

SGSDP: Sistema de Gestión de Seguridad de Datos Personales, sistema general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.

Sujeto obligado: Los sujetos obligados a que se refiere el artículo 1 de la (LGPDPPSO) que deciden sobre el tratamiento de datos personales.

Titular: La persona física a quien corresponden los datos personales.

Tratar el riesgo: Procesos que se realizan para modificar el nivel de riesgo.

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

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

Unidad de Transparencia: Área facultada para coordinar y vincular las acciones en materia de transparencia, acceso a la información y protección de datos personales y con las atribuciones conferidas en el artículo 67 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

Valorar el riesgo: Proceso para asignar valores a la probabilidad y consecuencias del riesgo.

Vulnerabilidad: Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

INTRODUCCIÓN

El ***Documento de Seguridad*** se refiere al 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. (Documento de seguridad versión 1.4. de agosto de 2016 elaborado por INAI).

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.

El artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados señala que el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

I. 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.

Así mismo el artículo 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas establece “El responsable deberá elaborar y aprobar un documento que contenga las medidas de seguridad de carácter físico, técnico y administrativo conforme a lo dispuesto en la presente Ley y demás disposiciones que resulten aplicables en la materia.

El documento de seguridad será de observancia obligatoria para los encargados y demás personas que realizan algún tipo de tratamiento de datos personales”.

En el Tribunal Superior de Justicia – Consejo de la Judicatura el ***DOCUMENTO DE SEGURIDAD*** se crea, a partir de la información que se genera, una vez que se han implementado las acciones en la construcción del Sistema de Gestión de Seguridad de Datos Personales (SGSDP), teniendo en su contenido lo siguiente:

- Relación de las instancias que integran la estructura de la institución y a las que aplica el SGSDP por tratar datos personales, (anexo 01).
- Asesorar a las instancias con el apoyo de las áreas técnicas a través de los Roles y Responsabilidades de los involucrados en el tratamiento de datos personales, (anexo 02).
- Las funciones y obligaciones de las personas que traten datos personales, ejemplos, (anexo 03).
- Catálogo de Tipos de Datos Personales, (anexo 04).
- El inventario de Datos Personales y de los sistemas de tratamiento, (anexo 05).
- Medidas de Seguridad de Datos Personales, (anexo 06).
- Análisis de riesgo de los datos personales, (anexo 07)
- El análisis de brecha, medidas de seguridad faltantes, (anexo 08)
- Plan de trabajo para la implementación de las medidas de seguridad faltantes, (anexo 09)
- La Vulneración de Datos Personales, (anexo 10)

- Programa General de Capacitación (anexo 11).
- De las Responsabilidades Administrativas y sus sanciones

En el contenido del ***Documento de Seguridad*** se cuenta con una relación de las ***instancias*** (anexo 01) que integran la estructura del Tribunal Superior de Justicia – Consejo de la Judicatura, la cual tiene una columna para que en ella se señale si la instancia de la que se verse, trata datos personales y que por lo tanto estará obligada a formar parte integrante del Sistema de Gestión de Seguridad de Datos Personales, (SGSDP).

Dentro de las políticas internas para la gestión y tratamiento de los datos personales se encuentran contemplados el asesoramiento a las instancias con el apoyo de las áreas técnicas, a través de los ***roles y responsabilidades específicas de los involucrados internos y externos dentro de la institución relacionados con los tratamientos de datos personales,*** (anexo 02)***;*** establecidos en la fracción II del artículo 56 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público y 51 de los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas; para cumplir con esta norma, se tiene diseñado el catálogo de áreas técnicas faltando establecer los nombres de los funcionarios titulares, éstas áreas técnicas fueron tomadas del documento del INAI llamado "Recomendaciones para el manejo de incidentes de seguridad de datos personales" y que será utilizado principalmente cuando sucedan incidentes y vulneraciones a la seguridad de los datos personales así como en el asesoramiento de las instancias.

Se integra en el documento una guía ***orientadora*** (no es vinculante), para definir ***las funciones y obligaciones de las personas que traten datos personales***, pudiendo los titulares de las instancias agregar o eliminar algunas funciones y obligaciones que consideren necesarias incluirlas en el inventario de datos personales, (anexo 03).

Con relación a lo previsto en el artículo 33, fracción III de la Ley General, 47, fracción III de la Ley Estatal y 58 fracción III de los Lineamientos Generales, establece que el responsable dentro la elaboración del inventario de datos personales también se deberá elaborar un catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no.

El objetivo es identificar qué tipo de datos personales se recaban en los distintos sistemas que se utilizan y lo más importante, valorar si es necesario recabarlos, cuya finalidad sea utilizar los datos necesarios para ser reflejados en los avisos de privacidad.

En el anexo 04, se encuentra el formato del catálogo de datos personales con el listado de los tipos de datos personales que hasta la fecha se tienen identificados para que las áreas puedan elegir cuales datos son necesarios para brindar los servicios.

Los documentos identificados como: ***"instancias"***, los ***"roles y responsabilidades específicas de los involucrados internos y externos dentro de la institución relacionados con los tratamientos de datos personales",*** la "***Guía de funciones y obligaciones"*** y el "***Catálogo de tipos de datos personales"*** servirán de apoyo para la elaboración del Inventario de Datos Personales.

EL INVENTARIO DE DATOS PERSONALES (anexo 05)

La elaboración del Inventario de Datos personales se encuentra contemplado en el Paso 4. Inventario de Tratamiento de Datos Personales del Sistema de Gestión de Seguridad de Datos Personales (SGSDP), teniendo como definición al control documentado de los tratamientos que realizan las instancias del Tribunal Superior de Justicia – Consejo de la Judicatura, elaborado con orden y precisión.

El inventario de datos personales al que hace referencia la Ley General en los artículos 33, fracción III, 35, fracción I; los artículos 47 fracción III, 50, fracción IV de la Ley Estatal; y 58 y 53 de los Lineamientos Generales y Estatales respectivamente, identifican los siguientes módulos relevantes:

Nombre de la Instancia, atribuciones para realizar el tratamiento, nombre del tratamiento y fundamento normativo para llevar a cabo del tratamiento.

Módulo I, Medios físicos y electrónicos a través de los cuales se obtienen los datos personales, pudiendo ser: presencial, telefónica, e-mail, internet, P.N.T., transferencias.

En caso de que la obtención sea mediante transferencia a través de un tercero, señalar el nombre de quien transfiere y las finalidades de la transferencia.

Módulo II, Finalidades de cada tratamiento de datos personales, indicando las finalidades, si se requiere consentimiento, supuesto señalado en el artículo 22 de la LGPDPSO y el tipo de consentimiento señalados en los Avisos de Privacidad.

Módulo III, Tipos de datos personales que se tratan, indicar el riesgo inherente que pueden ser bajo, medio, alto o muy alto y el nivel de riesgo que va del 1, 2, 3, al 4 o 5; anotando el nombre de los datos según el riesgo inherente y la finalidad del tratamiento de los datos.

Para que el titular de la instancia 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:

Riesgo inherente bajo, nivel de riesgo 1:

Datos identificativos: Nombre, Alias, Seudónimo o cualquier sobrenombre, Sexo, Estado Civil, Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Credencial de Elector (INE), Número de S.S., Cartilla Militar, Pasaporte, Licencia de Manejo, Acta de Nacimiento, Lugar de Nacimiento, Fecha de Nacimiento, Nacionalidad, Domicilio Particular, Domicilio (fiscal) del principal asiento de su negocio, Domicilio para oír y recibir notificaciones, Teléfono Particular, Teléfono Celular, Firma Autógrafa, Edad, Fotografía, Datos Familiares, Nombre de los Progenitores, Nombre de quien detenta la Patria Potestad, Dependientes Económicos.

Datos sobre características físicas: Color de Piel, Color de Iris, Color de Cabello, Señas particulares, Estatura, Peso, Cicatrices, Tipo de Sangre, Discapacidad.

Riesgo inherente medio, nivel de riesgo 2:

Datos de direcciones electrónicas: Correo Electrónico, Dirección IP, Dirección Mac, Nombre de Usuario, Contraseñas o Password, Firma Electrónica, Nombre de Usuario en Redes Sociales.

Datos laborales: Reclutamiento, Selección, Fecha de Ingreso, Enlace Plaza Adscripción, Categoría, Nombre de la Institución, Domicilio de Trabajo, Teléfono Institucional, Correo Electrónico Institucional, Referencias Laborales, Referencias Personales, Solicitud de Empleo, Experiencia/Capacitación, Actividades Extracurriculares, Registro en el Padrón de Contratistas, Acta Constitutiva, Estados Financieros.

Datos patrimoniales y/o financieros: Bienes Muebles, Bienes Inmuebles, Información Fiscal, Historial Crediticio/Buró de Crédito, Egresos, Cuentas Bancarias, Números de Tarjetas de Crédito, Información Adicional de Tarjeta (fecha de vencimiento, códigos de seguridad, datos de banda magnética, pin), Seguros, Fianzas, Afores, Clabe Interbancaria, Prestamos, Plazo para Reintegrar.

Datos legales: Persona sujeta a procedimiento administrativo, sujeta a juicio en materia laboral, sujeta a juicio en materia laboral, sujeta a juicio en materia civil, sujeta a juicio en materia familiar, sujeta a juicio en materia penal, sujeta a juicio en materia fiscal, sujeta a juicio en materia administrativa.

Datos Académicos: Grado máximo de estudios o Trayectoria educativa, Calificaciones, Títulos, Cédula Profesional, Certificados, Reconocimientos, Idiomas, Currículum vitae.

Riesgo inherente alto, nivel de riesgo 3:

Datos migratorios: Entrada al País, Salida del País, Tiempo de permanencia en el País, Calidad Migratoria, Derechos de Residencia, Aseguramiento, Repatriación.

Datos de salud: Expediente Clínico, descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, uso de aparatos ortopédicos, uso de aparatos auditivos, uso de prótesis, estado físico o mental, información genética (ADN).

Datos biométricos: Imagen de iris o retina, huella dactilar, palma de la mano.

Datos sobre pasatiempos: Entretenimiento y diversión, pasatiempos, aficiones, deportes que practica, juegos de su interés.

Riesgo inherente muy alto, nivel de riesgo 4 o 5:

Nivel de protección especial: Pertenencia a un pueblo, Etnia o región, Raciales, sobre la ideología, sobre convicciones religiosas, sobre convicciones morales, sobre convicciones filosóficas, pertenencia a un partido, opiniones políticas, pertenencia a un sindicato, preferencias sexuales, prácticas o hábitos sexuales, datos personales de la niñez.

Módulo IV: Almacenamiento físico y/o electrónico de los datos personales indicando si el tipo de soporte es físico, electrónico o de otro tipo de soporte.

Para lograr lo anterior, es preciso referirse a las definiciones que se prevén en las recomendaciones emitidas por el órgano garante:

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 (CD’s y DVD’s), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil.

Módulo V, Servidores Públicos que tienen acceso a los sistemas de tratamiento.

Responsable: (funcionario titular de la instancia): nombre, cargo, funciones y obligaciones.

Enlace: (persona designada por el responsable para la administración y custodia de los datos personales), se recomienda que sea la persona registrada en el Archivo Judicial como el responsable del Archivo de Trámite, anotando el nombre, cargo, funciones y obligaciones.

Usuario: (persona que, por sus actividades laborales y atribuciones legales, tiene acceso a los datos personales), anotando nombre, cargo, funciones y obligaciones de tantas personas como sean necesarias nombrarlas por el titular de la instancia, dadas las características de la institución.

NOTA: El formato tiene capacidad para siete (7) usuarios que tienen acceso a los datos personales, en caso de que la instancia cuente con más usuarios, pue de utilizarse el formato adicional previsto para estos casos.

Módulo VI, en su caso, el nombre completo o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable y señalar si el encargado realiza transferencias.

Módulo VII, en su caso, toda transferencia de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado; a los destinatarios o terceros receptores de las que se efectúen, así como las finalidades que la justifican, debiendo señalar: Nombre o Razón Social, finalidades de la transferencia, consentimiento para la transferencia S/N, supuestos señalados en los artículos 22, 66 o 70 de la Ley General, tipo de consentimiento que se requiere, suscripción de cláusulas contractuales y supuesto del artículo 66 de la Ley General que se actualiza.

Considerar en el inventario el ciclo de vida de los datos personales, conforme a lo siguiente:

- El bloqueo de los datos personales en el archivo de concentración, en su caso, y
- La cancelación, supresión o destrucción de los datos personales.

El almacenamiento de los Datos Personales, indicando si es en las instalaciones de la Instancia o en instalaciones de terceros.

Medios de almacenamiento de los datos personales electrónicos, indicando si son en computadoras pc, laptops, servidores propios, teléfonos inteligentes, tabletas, memorias usb, discos duros extraíbles, cd, dvd, blu-ray, cómputo en la nube.

Medios de almacenamiento físico, indicando si son en escritorios, anaqueles, cajas fuertes, carpetas, cajones, archiveros, bóvedas, folders.

Bloqueo de los datos personales, una vez que hayan dejado de ser útiles para los fines para los cuales fueron recabados, utilizando términos de clasificación archivísticos como los son:

Sección, señalar la clave y el nombre que le haya asignado el Catálogo de Clasificación Archivística diseñado por el Archivo Judicial de acuerdo a la norma señalada por la Ley General de Archivos.

Serie, señalar la clave y el nombre que le haya asignado el Catálogo de Clasificación Archivística diseñado por el Archivo Judicial de acuerdo a la norma señalada por la Ley General de Archivos.

Subserie, señalar la clave y el nombre que le haya asignado el Catálogo de Clasificación Archivística diseñado por el Archivo Judicial de acuerdo a la norma señalada por la Ley General de Archivos.

Años de conservación en el archivo de trámite, señalar el tiempo de conservación que se deben resguardar una vez que hayan dejado de ser útiles en el archivo de trámite.

Años de conservación en el archivo de concentración (archivo judicial), señalar el tiempo de guarda precaucional en el archivo de concentración.

Total, de años para determinar el borrado seguro de los datos personales según las directrices del INAI y de la Ley General de Archivos, resultado de la suma de los años de guarda en el Archivo de Trámite y en el Archivo de Concentración.

MEDIDAS DE SEGURIDAD DE DATOS PERSONALES (anexo 06)

Uciel Fragoso Rodríguez, cita en el Diccionario de Protección de Datos Personales lo siguiente:

Las medidas de seguridad son elementos de control que tienen el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información. En el caso de los datos personales, las medidas de seguridad se implementan a lo largo de su ciclo de vida para evitar que los datos sean expuestos, alterados o bloqueados por personas o entidades no autorizadas, (termina la cita).

Uno de los mayores retos a los que se enfrentan las instituciones hoy en día, es planear y prepararse para lo inesperado, especialmente para los incidentes que comprometen los servicios que ofrecen, así como la información que resguarda el responsable, inclusive los datos personales, poniendo en riesgo a su titular.

Alguno de los incidentes más comunes son los siguientes:

➢ Robo de información en documentos y medios de almacenamiento desechados incorrectamente.

➢ Empleados que acceden a datos personales sin la autorización correspondiente.

➢ Empleados que revelan información a otras personas a través de engaños.

➢ Robo o pérdida de equipos de cómputo, laptops, teléfonos inteligentes, tabletas, o memorias extraíbles con información personal.

➢ Acceso ilegal a las bases de datos personales por un externo a la organización.

En materia de seguridad de datos personales pueden abordarse bajo las siguientes categorías generales:

A) Medidas de seguridad administrativas, (Medidas basadas en la cultura del personal.)

Son el conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales.

Las medidas de seguridad administrativas son las políticas y procedimientos para la gestión, declaración de confidencialidad, clasificación de los archivos físicos, clasificación de los archivos electrónicos, capacitación, bitácora de consulta, bitácora de vulneraciones, depuración y borrado seguro del archivo físico, depuración y borrado seguro del archivo electrónico, transferencias.

B) Medidas de seguridad físicas, (Medidas en el entorno de trabajo físico).

Se refiere a las acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para:

a) Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información;

b) Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones;

c) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, integridad y confidencialidad, y

d) Garantizar la eliminación de datos de forma segura.

Conforme los equipos de cómputo son cada vez más pequeños, ligeros y convenientes se vuelve muy fácil para las personas llevar información con ellos, por otro lado, para muchas organizaciones es común revisar información en lugares públicos como un restaurante, cafetería o en el transporte público. La seguridad del entorno de trabajo físico es un elemento básico para mitigar vulneraciones a la seguridad de los datos personales.

C) Medidas de seguridad técnicas, (Medidas en el entorno de trabajo digital).

Son las actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:

a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados;

b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Se incluyan acciones para la adquisición¸ operación, desarrollo y mantenimiento de sistemas seguros;

d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales;

e) Cuidado de la contraseña personal;

f) Actualización de contraseñas;

g) Reporte de fallas;

h) No instalar softwares de dudosa procedencia;

i) Diseñar contraseñas robustas;

j) Respaldo de la información;

k) Otras

Se pueden determinar las medidas de seguridad aplicables a los datos personales que se tratan considerando los siguientes factores:

a) El riesgo inherente por tipo de dato personal;

b) La sensibilidad de los datos personales tratados;

c) El desarrollo tecnológico, y

d) Las posibles consecuencias de una vulneración para los titulares.

Además, se debe tomar en cuenta los siguientes elementos:

a) El número de titulares;

b) Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;

c) El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y

d) Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.

Muchas de las operaciones de las instituciones y de los mismos titulares de datos están siendo llevadas a entornos digitales, por lo que se vuelve primordial proteger equipos de cómputo y dispositivos de almacenamiento contra el acceso no autorizado, de igual forma, contra amenazas informáticas como software malicioso (malware, virus, entre otros).

Para tratar los temas señalados los responsables y encargados del tratamiento de datos personales deberán contestar la encuesta que forma parte de este documento respondiendo con una “S” o una “N”, a las preguntas que se plantean en el cuestionario de las Medidas de Seguridad Implementadas del anexo 06, este formato de encuesta fue tomado del “Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas Junio 2014 elaborado por el IFAI actualmente INAI.”

La encuesta una vez completada con cualquiera de las letras "**S**" o "**N**", deberá ser enviada a la Unidad de Transparencia para que se formule el Análisis de Brecha para que de manera conjunta y acumulada con las instancias que integran el Sujeto Obligado "Tribunal Superior de Justicia – Consejo de la Judicatura", dé como resultado el Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.

ANALISIS DE RIESGO DE LOS DATOS PERSONALES (anexo 07)

El proceso de análisis de riesgos considera la evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño. Contempla la identificación de activos, el estudio de causas y consecuencias de las amenazas y vulnerabilidades en los sistemas de tratamiento de datos personales, y permite establecer parámetros para ponderar los efectos de posibles vulneraciones de seguridad.

Esta metodología en particular, contempla tres factores que en conjunto determinan el riesgo latente de los datos personales:

Beneficio, factor que deriva en el nivel de riesgo por tipo de dato, determinado por el riesgo inherente del dato y el volumen de titulares de las que se tratan datos.

Accesibilidad, factor que determina el nivel de riesgo por tipo de acceso, es decir, el número de accesos potenciales a los datos.

Anonimidad, factor que determina el nivel de riesgo por tipo de entorno desde el que se tiene acceso a los datos.

Estos factores de riesgo nos permiten obtener un valor cuantitativo del nivel de riesgo latente de cada particular con relación al tratamiento de datos personales y sensibles y, a partir de ello, una lista de controles congruentes para disminuir los posibles impactos a los datos personales o sensibles.

A partir de lo anterior, se ha dado el nombre de "**BAA**" a esta metodología de análisis de riesgos, lo cual tiene su origen en el **B**eneficio para el atacante, la **A**ccesibilidad para el atacante y la **A**nonimidad del atacante.

TIPO DE LOS DATOS PERSONALES.

Los métodos para determinar el nivel de medidas de seguridad que deben adoptarse están establecidos en el catálogo de datos personales (anexo 04), a continuación se detallan algunos parámetros de clasificación:

Datos identificativos, *(Riesgo inherente bajo, nivel de riesgo 1)*: Nombre, Alias, Seudónimo o cualquier sobrenombre, Sexo, Estado civil, Registro federal de contribuyentes (RFC), Clave única de registro de población (CURP), Credencial de Elector (INE), Número del I.M.S.S., Cartilla Militar, Pasaporte, Licencia de manejo, Acta de Nacimiento, Lugar de nacimiento, Fecha de nacimiento, Nacionalidad, Domicilio Particular, Domicilio Fiscal, Domicilio para oír y recibir notificaciones, Teléfono particular, Teléfono celular, Firma autógrafa, Edad, Fotografía, Datos Familiares, Nombre de los Progenitores, Nombre de quien detenta la Patria potestad, Dependientes Económicos.

Datos sobre características físicas, *(Riesgo inherente bajo, nivel de riesgo 1)*: color de piel, color de iris, color de cabello, señas particulares, estatura, peso, cicatrices, tipo de sangre, discapacidad.

Datos electrónicos, (Riesgo inherente medio, nivel de riesgo 2): Correo electrónico, dirección IP, dirección Mac, nombre de usuario, contraseñas o password, firma electrónica, nombre de usuario en redes sociales.

Datos laborales, (Riesgo inherente medio, nivel de riesgo 2): Reclutamiento, selección, fecha de ingreso (R.H.), enlace (R.H.), plaza (R.H.), adscripción (R.H.), categoría (R.H.), nombre de la Institución (R.H.), domicilio de trabajo (R.H.), teléfono institucional (R.H.), correo electrónico institucional, referencias laborales, referencias personales, solicitud de empleo, experiencia/capacitación, actividades extracurriculares, registro en el padrón de contratistas, acta constitutiva, estados financieros

Datos patrimoniales y financieros, (Riesgo inherente medio, nivel de riesgo 2): bienes muebles, bienes inmuebles, información fiscal, historial crediticio/buró de crédito, ingresos, egresos, cuentas bancarias, números de tarjeta de crédito, información adicional de tarjeta (fecha de vencimiento, códigos de seguridad, datos de banda magnética, pin), seguros, fianzas, afores, clabe interbancaria, prestamos (R.H.), plazo para reintegrar (R.H.).

Datos legales, (Riesgo inherente medio, nivel de riesgo 2): persona sujeta a procedimiento administrativo, persona sujeta a juicio en materia laboral, persona sujeta a juicio en materia civil, persona sujeta a juicio en materia familiar, persona sujeta a juicio en materia penal, persona sujeta a juicio en materia fiscal, persona sujeta a juicio en materia administrativa.

Datos académicos, (Riesgo inherente medio, nivel de riesgo 2): grado máximo de estudios o trayectoria educativa, calificaciones, títulos, cédula profesional, certificados, reconocimientos, idiomas, currículum vitae.

Datos migratorios, (Riesgo inherente alto, nivel de riesgo 3): entrada al país, salida del país, tiempo de permanencia en el país, calidad migratoria, derechos de residencia, aseguramiento, repatriación.

Datos sobre la salud, (Riesgo inherente alto, nivel de riesgo 3): Expediente clínico, descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, uso de aparatos ortopédicos, uso de aparatos auditivos, uso de prótesis estado físico o mental.

Datos biométricos, (Riesgo inherente alto, nivel de riesgo 3): Imagen de iris o retina, huella dactilar, palma de la mano, información genética (ADN).

Datos sobre pasatiempos, entretenimiento y diversión, *(Riesgo inherente alto, nivel de riesgo 3):* Pasatiempos, aficiones, deportes que practica, juegos de su interés.

Datos sensibles especialmente protegidos, *(Riesgo inherente muy alto, nivel de riesgo 4-5):* Pertenencia a un pueblo, etnia o región, datos raciales, datos sobre la ideología, datos sobre convicciones religiosas, datos sobre convicciones morales, datos sobre convicciones filosóficas, pertenencia a un partido/opiniones políticas, pertenencia a un sindicato, preferencias sexuales, prácticas o hábitos sexuales.

ADVERTENCIA: Los datos señalados en el catálogo son susceptibles de hacerse públicos, primero cuando por ley exista una obligación de difundirlos y segundo cuando se trate de servidores públicos, tal es el caso de algunos datos identificativos, patrimoniales, laborales, académicos, etcétera.

NIVELES DE RIESGO

Las medidas de seguridad que deberán adoptarse por el responsable deben tomar como referencia el nivel de riesgo que presenta cada tratamiento de datos personales. Para ello, es necesario calcular los factores de riesgo por ***tipo de dato***, por ***tipo de acceso*** y por ***entorno*** desde el cual se realizan los tratamientos de los datos personales.

A partir del tipo de dato es posible reconocer el factor de riesgo inherente, como se muestra a continuación:

TIPO DE DATO	RIESGO INHERENTE	NIVEL DE RIESGO
Datos identificativos; características físicas	**Bajo**	**1**
Datos electrónicos, laborales, patrimoniales, financieros, legales, académicos	**Medio**	**2**
Datos migratorios, salud, biométricos, pasatiempos, entretenimiento y diversión	**Alto**	**3**
Datos sensibles especialmente protegidos	**Muy alto**	**4 - 5**

Fuente "Documento de seguridad, aproximaciones institucionales", de la S.C.J.N.

Al riesgo inherente, se suma el volumen de titulares (personas) comprendidos en la base de datos, por ejemplo:

< 500: Datos de hasta 500 personas
< 5k: Datos entre 501 hasta 5,000 personas
< 50k: Datos entre 5,001 hasta 50,000 personas
< 500k: Datos entre 50,001 hasta 500,000 personas

El riesgo inherente más el volumen de titulares, da como resultado el nivel de riesgo por tipo de dato:

NIVEL DE RIESGO POR TIPO DE DATO				
Tipo de dato/número de titulares	**< 500**	**< 5k**	**< 50k**	**< 500k**
Datos sensibles especialmente protegidos	**4**	**4**	**5**	**5**
Datos migratorios, salud, biométricos, pasatiempos, entretenimiento y diversión	**1**	**2**	**3**	**3**
Datos electrónicos, laborales, patrimoniales, financieros, legales, académicos	**1**	**1**	**2**	**2**
Datos identificativos; características físicas	**1**	**1**	**1**	**1**

Fuente "Documento de seguridad, aproximaciones institucionales", de la S.C.J.N.

El nivel de riesgo por tipo de dato servirá para determinar los controles que se deben considerar para su protección.

Por otra parte, el riesgo por tipo de acceso se mide determinando la cantidad de accesos potenciales a los datos personales que se pretenden proteger en un intervalo de tiempo, por ejemplo, durante 10 horas. Para este parámetro entre mayor sea la accesibilidad, mayor riesgo existe para la información.

ACCESIBILIDAD (CANTIDAD DE ACCESOS)	VALOR
< 10	1
< 20	2
< 30	3
< 40	4

Fuente "Documento de seguridad, aproximaciones institucionales", de la S.C.J.N.

El riesgo por tipo de entorno, este factor representa el nivel de anonimidad para acceder o hacer uso de los datos personales que se tratan. Entre mayor anonimidad ofrezca el entorno, mayor riesgo existe de que se vulnere la seguridad.

ENTORNO	NIVEL DE RIESGO
Físico	1
Equipo de cómputo	2
Nube	3
Internet	4

Fuente "Documento de seguridad, aproximaciones institucionales", de la S.C.J.N.

En caso de que se accedan por más de un entorno a los datos personales, se debe considerar el entorno de mayor riesgo.

La combinación de los tres factores analizados da como resultado el nivel de riesgo latente de cada tratamiento de datos personales, lo cual contribuye a identificar el nivel de medidas de seguridad que deben implementarse en cada caso.

Una vez que se calcula el nivel de riesgo latente por cada tratamiento de datos personales, es posible realizar estrategias para identificar los modelos de medidas de seguridad que deben aplicarse a cada uno de ellos.

EJEMPLO DE NIVEL DE RIESGO DEL GRUPO DE DATOS IDENTIFICATIVOS:

NIVELES DE RIESGO	VALOR
Nombre = Datos identificativos: (Riesgo inherente bajo, Nivel de riesgo (1))	1
Volumen de titulares de datos personales en la base de datos <500	1
Accesos a los datos personales durante 12 horas < o = 10	1
Nivel de anonimidad (entorno) físico, para acceder o hacer uso de los datos personales	1
VALOR que tiene el NOMBRE de un titular de sus datos personales en caso de un incidente	4

EJEMPLO DE NIVEL DE RIESGO DEL GRUPO DATOS PERSONALES SENSIBLES ESPECIALMENTE PROTEGIDOS:

NIVELES DE RIESGO	VALOR
Pertenencia a un pueblo, etnia o región = Datos sensibles: (Riesgo muy alto, Nivel de riesgo (4 o 5))	4
Volumen de titulares de datos personales en la base de datos <500	4
Accesos a los datos personales durante 12 horas < 20	2
Nivel de anonimidad (entorno) físico, para acceder o hacer uso de los datos personales	1
VALOR que tiene el dato sensible de la PERTENCIA A UN PUEBLO, ETNIA O REGIÓN de un titular de los datos personales en caso de un incidente	11

PROPÓSITO DEL ANÁLISIS DE RIESGO

Realizar un análisis de riesgos por cada tratamiento ayudará a identificar el nivel de medidas de seguridad que deben ser implementadas para la protección de los datos personales.

El análisis de riesgo deberá ser implementado por todas las instancias que traten datos personales por medio de una encuesta cuyo formato se encuentra en el anexo 07.

EL ANÁLISIS DE BRECHA, MEDIDAS DE SEGURIDAD FALTANTES (anexo 08)

El análisis de brecha se puede definir como la concentración de elementos específicos que pueden existir entre lo deseable y lo actual, para ello es importante definir con claridad cuál es la brecha que se desea analizar, identificar quiénes están involucrados, establecer cuáles son las causas más relevantes que determinan la brecha, identificar las diferencias de comportamiento entre los sistemas o actores a comparar en la brecha, identificar los indicadores y/o atributos de la situación actual y elaborar un listado con la finalidad de medir o caracterizar la brecha.

En síntesis, el análisis de brecha debe aportar lo contenido en los Lineamientos Generales de Protección de Datos Personales para el Sector Público, que en el artículo 61 (con relación al artículo 33, fracción V de la LGPDPPSO) establece que para la realización del análisis de brecha, el responsable deberá considerar las medidas de seguridad existentes y efectivas, las medidas de seguridad faltantes y la existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente. **(Diccionario de Protección de Datos Personales).**

Este análisis es indispensable en cualquier Programa de Protección de Datos Personales dado que permite identificar las medidas de seguridad actualmente implementadas, evaluar su efectividad en el tratamiento de los riesgos resultantes del proceso de análisis de riesgos.

Además, permite definir nuevas medidas de seguridad para atender los riesgos, reforzando con ello la protección de los datos personales.

Una vez identificados los activos y procesos relacionados con los datos personales, así como las amenazas, vulnerabilidades y escenarios de incidentes, se debe proceder al análisis de brecha.

El análisis de brecha consiste en identificar:

- Las medidas de seguridad existentes.
- Las medidas de seguridad existentes que operan correctamente.
- Las medidas de seguridad faltantes.

En el anexo 08 se encuentra el formato de Encuesta de Análisis de Brecha el cual debe ser llenado en la instancia que trate datos personales, este formato de encuesta para el Análisis de Brecha, fue tomado del “Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas Junio 2014 elaborado por el IFAI actualmente INAI.”

La encuesta una vez completada con cualquiera de las letras “**S**” o “**N**”, deberá ser enviada a la Unidad de Transparencia para que se formule el Análisis de Brecha de la instancia y de manera conjunta y acumulada por las demás instancias que integran el Sujeto Obligado “Tribunal Superior de Justicia – Consejo de la Judicatura”, dé como resultado el Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.

PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE LAS MEDIDAS DE SEGURIDAD FALTANTES (anexo 09)

El plan de trabajo se elaborará para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

Este plan de trabajo deberá elaborarse de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Se deben seleccionar los controles de seguridad faltantes identificados en el análisis de brecha y en el plan de tratamiento del riesgo, tomando en cuenta la ponderación hecha en la valoración.

Existen cuatro posibilidades comunes para tratar el riesgo:

1.- Mitigar o reducir el riesgo.
2.- Retener el riesgo.
3.- Evitar el riesgo.
4.- Compartir el riesgo.

Las opciones de tratamiento del riesgo serán seleccionadas con base en el resultado de la valoración del riesgo, los costos estimados, y los beneficios esperados de implementar estas opciones.

Si se obtiene una considerable reducción del riesgo con un costo relativamente bajo, esto es una combinación a considerar para implementar los controles. En general, las consecuencias adversas de los riesgos deben reducirse lo más razonablemente posible con independencia de cualquier criterio absoluto, por ejemplo, se deben considerar los riesgos que no ocurren con frecuencia pero que serían severos, en cuyo caso también se deben implementar controles.

Los cuatro tipos de tratamiento de riesgo no son mutuamente excluyentes, a veces las organizaciones pueden beneficiarse sustancialmente de la combinación de opciones, como reducir la probabilidad de un riesgo, reducir sus consecuencias, compartir o retener el riesgo residual.

Algunos tratamientos pueden atender a más de un riesgo, por ejemplo, el entrenamiento y concienciación del personal. El plan de tratamiento del riesgo tiene que establecer prioridades de atención de riesgos específicos y su periodo, dicha prioridad puede establecerse equilibrando la valoración del riesgo y el análisis costo-beneficio de la implementación en relación con el presupuesto.

Finalmente, el plan de trabajo se podrá elaborar, hasta que el sistema de gestión de seguridad de datos personales (SGSDP) se encuentre en pleno funcionamiento como resultado de las medidas de seguridad faltantes.

Lo anterior, considerando:

- Los recursos designados;
- El personal interno y externo, y
- Las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

En la página siguiente se ilustra el formato del Plan de Trabajo

PLAN DE TRABAJO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES
TRIBUNAL SUPERIOR DE JUSTICIA – CONSEJO DE LA JUDICATURA DEL ESTADO DE CHIAPAS

En este documento se describen las actividades relacionadas con la implementación de las medidas de seguridad recomendadas para los tratamientos de datos personales, de conformidad con el resultado del análisis de brecha elaborado por cada una de las instancias que integran el sujeto obligado y consolidado por el área de protección de datos personales de la Unidad de Transparencia, en cumplimiento del artículo 35 fracción V de la Ley General y el artículo 47 fracción VI de la Ley Estatal.

MEDIDA FALTANTE	CATEGORIA	DESCRIPCIÓN DE LA ACTIVIDAD	INSUMOS O FORMAS DE IMPLEMENTACIÓN	INSTANCIAS INVOLUCRADAS

PLAN DE TRABAJO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES
TRIBUNAL SUPERIOR DE JUSTICIA – CONSEJO DE LA JUDICATURA DEL ESTADO DE CHIAPAS

INSTRUCTIVO PARA LA FORMULACIÓN DEL PLAN DE TRABAJO

(01) = MEDIDA FALTANTE.- Anotar en esta columna la descripción de la medida de seguridad faltante.
(02) = CATEGORIA.- Anotar la categoría de la medida de seguridad ADMINISTRATIVAS, FÍSICAS O TÉCNICAS.
(03) = DESCRIPCIÓN DE LA ACTIVIDAD.- Anotar la descripción los más sucinta posible pero que sea posible interpretar la actividad a desarrollar
(04) = INSUMOS O FORMAS DE IMPLEMETACIÓN.- Describir los insumos (materiales, reparaciones, gastos, etc.)
(05) = INSTANCIAS INVOLUCRADAS.- Anotar el nombre de las áreas que intervienen en el desarrollo de los trabajos, ejemplo: (Recursos Materiales, Construcción, Infraestructura Tecnológica, etc.)

MEDIDA FALTANTE	CATEGORIA	DESCRIPCIÓN DE LA ACTIVIDAD	INSUMOS O FORMAS DE IMPLEMENTACIÓN	INSTANCIAS INVOLUCRADAS
(01)	(02)	(03)	(04)	(05)

VULNERACIÓN DE DATOS PERSONALES

PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD

La gestión de incidentes es el proceso de planeación, comunicación y capacidad de acción cuando ocurre un incidente de seguridad. Por lo tanto, elaborar un plan de respuesta a incidentes es probablemente una de las tareas más complejas en seguridad de la información.

Por lo anterior, en este apartado se presenta el documento de Bitácora de Vulneraciones de Datos Personales para atender incidentes de seguridad, a fin de prevenir y mitigar las vulneraciones a la seguridad de los datos personales.

Los activos, las amenazas y las vulnerabilidades se combinan para generar riesgos. Cuando un riesgo se materializa, ocurre un incidente de seguridad, el cual se traduce en una violación a las medidas de seguridad.

RIESGO = Amenaza que genera una acción o evento no deseado y que trata de explotar vulnerabilidades de los archivos

"Un incidente de seguridad es un riesgo materializado"

Para identificar un incidente de seguridad, se requiere de la detección y/o registro de alertas de seguridad, los cuales son advertencias respecto a cambios en los sistemas de tratamiento.

Sin embargo, dichas alertas no siempre implican que haya ocurrido un incidente de seguridad. Además, si no se tienen suficientes medidas de seguridad, puede ocurrir un incidente sin que éste se detecte.

A continuación, se presenta una lista de alertas de seguridad, que pueden advertir de una anomalía o cambio no deseado en los activos:

EJEMPLOS DE ALERTAS DE SEGURIDAD	
ENTORNO	**TIPO DE ALERTA**
FÍSICO	Alarmas para desastres como incendios o terremotos.
	Alarmas automatizadas contra robos o intrusos en instalaciones.
	Alertas del personal de vigilancia o a través de circuito cerrado de video.
	Aviso de desaparición o extravío de equipos de cómputo, medios de almacenamiento o documentos.
	Avisos del personal, justiciables, proveedores, autoridades o reportes en medios de comunicación masivos.
	Anomalías o accesos no autorizados identificados en bitácoras de los sistemas de tratamiento físicos.
EJEMPLOS DE ALERTAS DE SEGURIDAD	
ENTORNO	**TIPO DE ALERTA**
ELECTRÓNICO	Notificaciones sobre software malicioso o vulnerabilidades técnicas descubiertas, preferentemente de fuentes confiables como agencias nacionales o firmas especializadas en riesgos o seguridad.
	Alertas de sistemas automatizados como firewalls, antivirus, filtros de contenido, sistemas de detección de intrusos (IDS = Intrusion Detection System, por sus siglas en inglés) o gestores de seguridad de la información y eventos (SIEM = Security Information and Event Management, por sus siglas en inglés).
	Anomalías o accesos no autorizados identificados en bitácoras de los sistemas de tratamiento automatizados, medios de almacenamiento y equipos de cómputo.

Cuando se identifica o reporta una alerta de seguridad que involucra información comprometida o daño a los activos, **se habla de un incidente de seguridad.**

En la siguiente tabla se enlistan diferentes categorías de incidentes de seguridad:

ALERTAS DE SEGURIDAD	
CATEGORÍA	**EJEMPLOS DE ALERTAS**
Desastre natural (más allá del control humano)	Terremoto, erupción de un volcán, tsunami, huracán, etc.
Inestabilidad social	Huelgas, terrorismo, guerra.
Daño físico (accidental o deliberado)	Incendio, inundación, malas condiciones ambientales (contaminación, polvo, corrosión, congelamiento), radiación o pulso electromagnético, destrucción parcial o toral de medios de almacenamiento físico o electrónico.
Falla de la infraestructura	Falla en el suministro de servicios como: energía, agua, telecomunicaciones y redes, aire acondicionado.
Falla técnica	Fallas del hardware, mal funcionamiento del software, sobrecarga o saturación en el uso de los sistemas, falta de mantenimiento.
Software malicioso	Diferentes categorías de software malicioso (malware) como virus, troyanos, software de acceso y control remoto (RAT = espía, por sus siglas en inglés), amenazas persistentes avanzadas (APT = Advanced Persistent Threat, por sus siglas en inglés), Ransomware = software malicioso.
Ataques técnicos	Explotación de vulnerabilidades de la configuración, protocolos o programas, normalmente a la fuerza. Escaneo de redes, utilización de puertas traseras en el software, intentos de acceso no autorizado, inferencia de contraseñas, ataques de denegación de servicio.
Incumplimiento de reglas o políticas (accidental o deliberado)	Uso no autorizado de activos, uso de activos autorizados, pero para finalidades no autorizadas, uso de software, o dispositivos no permitidos, instalación de programas o aplicaciones no autorizadas o ilegales, copia o sustracción de documentos o información no autorizada.
Información dañada	Sobre escritura accidental, error de captura o de almacenamiento.
Intercepción de información	Espionaje, intervención de comunicaciones, ingeniería social, robo, pérdida o extravío de información.
Divulgación de contenido perjudicial	Difusión en medios masivos de comunicación de contenido ilegal, malicioso, abusivo o que pueda dañar los derechos morales o patrimoniales de las personas.

En suma, un riesgo materializado es un incidente, y se detecta a través de las alertas de seguridad, como se puede observar en la definición siguiente:

Relación entre riesgos, incidentes y alertas de seguridad

Riesgo materializado es un Incidente de seguridad que se detecta a través de una alerta de seguridad

INCIDENTES DE SEGURIDAD QUE AFECTAN DATOS PERSONALES

Por su parte, las vulneraciones a la seguridad de los datos personales o vulneraciones de seguridad, mencionadas en los artículos 41 de la Ley General y 55 de la Ley Estatal, son un tipo particular de incidente de seguridad que se caracterizan por:

a) Afectar a los activos o sistemas relacionados con los datos personales, en cualquier fase de su tratamiento.

b) Afectar de manera significativa los derechos patrimoniales o morales de los titulares de los datos personales.

A su vez, derivado de una vulneración de seguridad, los responsables tienen el deber de analizar las causas por las cuales se presentó ésta, e implementar las medidas de seguridad preventivas y correctivas para evitar que incidentes similares se repitan.

a) Informar a los titulares de los datos personales lo siguiente:

1. La naturaleza del incidente.
2. Los datos personales comprometidos.
3. Las recomendaciones al titular acerca de las medidas que éste puede adoptar para protegerse.
4. Las acciones correctivas realizadas de forma inmediata.
5. Los medios donde los titulares pueden obtener más información.

b) Informar al ITAIPCH vulneración de seguridad ocurrida.

c) La actualización del documento de seguridad correspondiente.

d) Contar con una bitácora de las vulneraciones en la que se describa:

1. En qué consistió la vulneración.
2. La fecha en la que ocurrió.
3. El motivo o causa de la vulneración.
4. Las acciones correctivas implementadas de forma inmediata y a largo plazo.

e) La imposición de sanciones por la autoridad correspondiente debido a la falta de implementación de medidas de seguridad.

"Las vulneraciones a la seguridad de los datos personales son incidentes de seguridad"

Finalmente, las revelaciones son incidentes de seguridad que exponen la información a través de Internet o en medios masivos de comunicación. Las revelaciones de información pueden resultar en una vulneración de seguridad al exponer datos personales a un sinnúmero de terceros.

Cuando se identifica que una revelación expone datos personales, el responsable debe tomar todas las medidas que estén a su alcance para mitigar la difusión o publicación de los mismos. Por ejemplo, solicitar la baja de contenido al administrador de una página web, así como pedir la eliminación de resultados de un motor de búsqueda, a fin de minimizar el daño a los titulares.

De esta manera, es posible observar que las vulneraciones de seguridad son incidentes de seguridad que involucran datos personales, las cuales podrían resultar en revelaciones de información, como se muestra en la expresión siguiente:

Un incidente de seguridad que involucra datos personales es una vulneración de seguridad que expuesta en medios masivos es una revelación.

Un solo evento no siempre es un indicador de un incidente, por ello se tienen que revisar si hay otras notificaciones o alertas, o bien el equipo de respuesta a incidentes debe buscar otros indicadores que den muestra de que los activos han sido afectados. Entre más información se pueda recabar, existirá mayor certeza respecto a la naturaleza del incidente.

Existen alertas de seguridad cuya naturaleza refleja un incidente de manera evidente, y por lo tanto no requieren una investigación intensiva para pasar a la fase de contención. Por ejemplo, un evento en el que un empleado que de manera accidental derrama el café sobre documentos o equipo de cómputo, se puede catalogar de manera inmediata como un incidente.

Sin embargo, una vez que se identifica un incidente, siempre es necesario buscar alertas adicionales a la que detonó la identificación, para determinar su alcance total. Por ejemplo, derivado de una auditoría se tiene conocimiento que se han extraviado los expedientes en papel de un grupo de justiciables, esto ya es un evento que se puede catalogar como incidente, sin embargo, se tendría que realizar una revisión en el archivo a fin de identificar si otros expedientes han sido sustraídos.

En este punto se incluye un formato que deben utilizar los responsables como referencia para documentar y atender los incidentes de seguridad en sus instancias.

Cuando, derivado del seguimiento de un incidente de seguridad, se deban recabar datos personales, el responsable deberá presentar el aviso de privacidad correspondiente.

Dentro de las políticas internas para la gestión y tratamiento de los datos personales se encuentran contemplados el asesoramiento a las instancias con el apoyo de las áreas técnicas, a través de los ***roles y responsabilidades específicas de los involucrados internos y externos dentro de la institución relacionados con los tratamientos de datos personales,*** **(anexo 02)*;*** establecidos en la fracción II del artículo 56 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público y 51 de los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas; para cumplir con esta norma, se tiene diseñado el catálogo de áreas técnicas los cuales será actualizados con los nombres de los funcionarios titulares, éstas áreas técnicas fueron tomadas del documento del INAI llamado “Recomendaciones para el manejo de incidentes de seguridad de datos personales” y que será utilizado principalmente cuando sucedan incidentes y vulneraciones a la seguridad de los datos personales así como en el asesoramiento de las instancias.

Los titulares de las instancias que integran los roles y responsabilidades específicas de los involucrados *internos y externos dentro de la institución relacionados con los tratamientos de datos personales,* se detallan en el anexo 02 del presente documento y se refieren a los titulares de las siguientes instancias mediante el formato de lista de contactos el cual tiene la finalidad de crear un directorio de las personas o áreas clave con las que se debe mantener comunicación directa en caso de un incidente de seguridad.

Director(a) de la Unidad de Transparencia
Director(a) del Archivo Judicial
Director(a) Asuntos Jurídicos
Director(a) Desarrollo e Infraestructura Tecnológica
Jefe(a) del Departamento de Soporte Técnico
Contralor Interno
Titular de la Instancia involucrada (Magistrado, Juez, Director, etc.)
Director(a) de Recursos Humanos
Director(a) de Comunicación Social y Relaciones Públicas
Coordinador(a) de Protección Civil y Medio Ambiente
Coordinador(a) de Vigilancia y Seguridad
ITAIPCH / Autoridad en Materia de Protección de Datos Personales
Consejo de la Judicatura / Autoridad de la Institución

Se debe utilizar el formato de identificación de incidentes para documentar una o más alertas que se consideren relevantes o que se relacionen con un incidente de seguridad. El formato de identificación de incidentes se utiliza para dar seguimiento al acontecimiento, desde el usuario que reporta hasta el área que atiende la alerta.

BITÁCORA DE INCIDENTES (anexo 10)

Se debe utilizar el formato de ***identificación de incidentes*** para documentar una o más alertas que se consideren relevantes o que se relacionen con un incidente de seguridad.

El formato de identificación incidentes se utilizará para dar seguimiento al incidente, desde el usuario que reporta hasta el área que atiende la alerta y será la bitácora de vulneraciones.

Incidente de seguridad: Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas de un responsable, que afecte la confidencialidad, la integridad o la disponibilidad de la información.

FORMATO DE IDENTIFICACIÓN DE INCIDENTES

INFORMACIÓN GENERAL

(Para ser llenado por quien detecta el incidente)

Información del personal que detecta el incidente					
Nombre:					
Dirección:					
Teléfono:		Extensión:		Celular:	
Fax:		Correo electrónico:			

Información sobre el incidente:			
Fecha:		Hora:	
Localización donde se detectó el incidente:			

Tipo de sistema de tratamiento:	☐ Físico	☐ Electrónico

Nombre del responsable del sistema de tratamiento:	

Se encuentran involucrados datos personales en el incidente:	☐ Si	☐ No

Tipo de datos personales involucrados:	
Descripción de lo sucedido:	
Evaluación (para ser llenado por el equipo de gestión de incidentes)	

Una vez analizada la información, se determina que se trata de un incidente de seguridad:	☐ Si	☐ No

Justificación
Mencionar si existe algún posible impacto legal o contractual por el incidente:

RESUMEN DEL INCIDENTE (para ser llenado por el equipo de gestión de incidentes)

RESUMEN EJECUTIVO DEL INCIDENTE

RESUMEN TÉCNICO DEL INCIDENTE			
Tipo de Incidente	☐ Denegación de servicio	☐ Uso no autorizado	☐ Espionaje
	☐ Código malicioso	☐ Acceso no autorizado	☐ Robo, pérdida o extravío
	☐ Ingeniería social	☐ Otro: _____	

Sitio/Área/ Departamento donde se presentó el incidente:					
Nombre del contacto en el sitio donde se presentó el incidente:					
Dirección:					
Teléfono:		Teléfono alterno:		Celular:	
Fax:		Correo electrónico:			

¿Cómo fue detectado el incidente?

Información adicional

FIRMAS	
Nombre y firma del personal que detecta el incidente	Nombre y firma del personal representante del Equipo de Gestión de Incidentes

NOTIFICACIÓN DE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

La notificación de vulneraciones de seguridad es un requisito contemplado en la normativa mexicana en materia de protección de datos personales, para que los titulares de los datos personales puedan tomar medidas para la protección de sus derechos morales y patrimoniales.

La notificación al organismo garante (ITAIPCH), también es obligatorio.

En esta sección se desarrollarán algunas consideraciones que permiten a los responsables atender este deber adecuadamente.

BENEFICIOS DE LA NOTIFICACIÓN DE VULNERACIONES

Más allá del requerimiento legal, la notificación de vulneraciones debe considerarse como una medida de seguridad que ofrece múltiples beneficios:

- Puede ayudar a limitar el mal uso de los datos personales, ya que el mismo titular de los datos podría tomar acciones para su protección.
- Permite a los titulares de las unidades administrativas minimizar la pérdida de confianza de los titulares de los datos, al mostrar que cuando sufren una vulneración de seguridad, toman acciones para mitigar el impacto del incidente.
- Puede reducir los gastos de mitigación, al evitar la presentación de denuncias, y sus posibles sanciones, por falta de cumplimiento de la obligación legal de notificar la vulneración al titular de los datos y, en su caso, a la autoridad.

PROCESO DE NOTIFICACIÓN DE VULNERACIONES

La notificación de vulneraciones se debe realizar en el momento adecuado y con la información suficiente, para evitar la exposición de los sistemas de tratamiento y de cualquier otro activo, a fin de que los titulares de los datos puedan estar protegidos.

A continuación, se presentan las preguntas que un responsable tiene que hacerse para la adecuada notificación de vulneraciones:

1) ¿Cuándo notificar?

En general, se recomienda notificar a los titulares:

1. en el menor tiempo posible.
2. cuando ya se tenga información concreta del incidente.
3. cuando ya no exista exposición de los activos involucrados en la vulneración.

Dentro del proceso de respuesta a incidentes, esto ocurre al final de la etapa de contención, o bien al inicio de la etapa de mitigación.

“Dentro de la respuesta a incidentes, el final de la etapa de contención y el inicio de la etapa de mitigación son los mejores momentos para notificar una vulneración a la seguridad de los datos personales”

Los responsables de las unidades administrativas deberán notificar al titular de los datos y al ITAIPCH las vulneraciones de seguridad dentro de un plazo máximo de setenta y dos horas, a partir de que se confirme la ocurrencia de éstas y el responsable de la unidad administrativa haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación. Dicho plazo comenzará a correr el mismo día natural en que el responsable de la unidad administrativa confirme la vulneración de seguridad.

2) ¿Cómo notificar?

El método recomendado de notificación es el directo con los titulares de los datos, es decir por teléfono, correo electrónico, correo postal, o en persona. En caso de que exista urgencia por contactar al titular, puede resultar oportuno utilizar más de un medio de contacto a la vez.

Se puede optar por la notificación indirecta a través de sitios web o medios de comunicación masivos, solamente cuando la notificación directa pueda causar más afectaciones al titular, sea muy costosa o no se tenga información del contacto.

La notificación debe ser independiente y personalizada, y no debe incluir material o información no relacionada con el incidente de seguridad, ya que podría causar confusión.

3) ¿Quién debe notificar?

El responsable de la unidad administrativa del tratamiento de los datos personales, incluso si la vulneración ocurrió o involucró a un encargado (persona física o jurídica, pública o privada, ajena a la institución del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable).

4) ¿A quién se debe notificar además del titular de los datos personales?

Si derivado de la investigación de un incidente se identifica un posible delito, se debe dar parte al Ministerio Público.

Cuando un incidente resulte en una vulneración de seguridad, el responsable de la unidad administrativa de la que se trate tiene la obligación de informar al ITAIPCH, mediante escrito presentado en el domicilio, o bien a través de cualquier otro medio que se habilite para tal efecto, al menos lo siguiente:

a) La hora y fecha en que se identificó la vulneración.
b) La hora y fecha en que inició la investigación sobre la vulneración.
c) La naturaleza de la vulneración ocurrida.
d) La descripción detallada de cómo ocurrió la vulneración.
e) Los tipos de datos personales comprometidos y el número aproximado de titulares afectados.
f) Los sistemas de tratamiento comprometidos.
g) Las acciones correctivas realizadas de forma inmediata.
h) La descripción de las posibles consecuencias de la vulneración ocurrida.
i) Las recomendaciones dirigidas al titular.
j) El medio puesto a disposición del titular para que obtenga mayor información sobre la vulneración y cómo proteger sus datos personales
k) El nombre completo de la o las personas designadas para proporcionar mayor información al ITAIPCH, en caso de requerirse.
l) Cualquier otra información o documentación que considere conveniente hacer del conocimiento del ITAIPCH.

En algunos casos puede ser conveniente notificar a aseguradoras, instituciones financieras o a centros de respuesta a incidentes, para obtener asesoría o proporcionar a los titulares mayor apoyo.

5) ¿Qué se debe notificar a los titulares?

El contenido de una notificación a los titulares puede variar dependiendo de la vulneración ocurrida.

Sin embargo, la información que proporcione el responsable debe servir para que el titular entienda el incidente y pueda prevenir una mayor afectación, la notificación debe considerar al menos:

a) Descripción de la vulneración: se debe explicar de manera muy sencilla y general el incidente ocurrido, en qué consistió, así como el periodo en el que se desarrolló. No se deben dar detalles o incluir información que revele vulnerabilidades o fallas específicas en los sistemas de tratamiento.

b) Datos personales involucrados: una descripción de la información involucrada en el incidente.

c) Recomendaciones a los titulares: el listado de acciones que puede realizar el titular para minimizar los efectos adversos de la vulneración.

d) Acciones correctivas o de mitigación: una descripción general de las acciones llevadas a cabo para evitar que incidentes similares se repitan.

e) Información de contacto: datos de las áreas designadas, mesas de servicio o del personal de la institución que puede atender dudas y proporcionar información adicional del incidente.

f) Fuentes de información adicional: referencias o documentos adicionales de consulta para apoyar a los titulares ante situaciones específicas, como el robo de identidad, en su caso.

LOS MECANISMOS DE MONITOREO Y REVISIONES DE LAS MEDIDAS DE SEGURIDAD (sujeto al plan de trabajo de la Contraloría Interna)

LAS AUDITORÍAS

El documento Orientador de Protección de Datos Personales señala que dentro de las obligaciones del responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

Entre las actividades para el cumplimiento de esta disposición están:

Realizar al menos una auditoría integral al programa una vez al año.

Las auditorías deberán incluir la revisión del cumplimiento de las obligaciones que tiene el Comité de Transparencia en cuanto a la aplicación del SGSDP; evaluar la conformidad con el SGSDP; incluir, cuando sea posible, cifras, indicadores y estadísticas relacionadas con los procedimientos puestos en operación, y contener recomendaciones para hacer más efectivo y eficiente el cumplimiento del Programa.

Asimismo, se podrán llevar a cabo auditorías parciales cuando resulten necesarias para supervisar y monitorear el cumplimiento de obligaciones específicas en tratamientos particulares.

Como resultado de las auditorías se deberá obtener el nivel de madurez del sujeto obligado con relación a la protección de datos personales en su posesión, a fin de tenerlo como referencia y línea base para la mejora continua

En el caso de auditorías externas, el Comité de Transparencia deberá asegurar la objetividad e imparcialidad del auditor y el programa propuesto.

La instancia responsable del cumplimiento recae en la Contraloría Interna del Tribunal Superior de Justicia – Consejo de la Judicatura.

LAS REVISIONES ADMINISTRATIVAS

Las revisiones administrativas, las cuales deberán estar documentadas, tendrán como objetivo supervisar:

I) El adecuado desarrollo y efectividad del Programa, o bien,

II) El debido tratamiento en los cambios que afecten aspectos significativos en la protección de datos personales, como nueva normatividad, tecnología, o procesos o procedimientos.

Las revisiones administrativas deberán basarse en:

- La retroalimentación por parte de las instancias;
- Los riesgos identificados en el análisis de riesgos;
- Los resultados de auditorías;
- Los resultados de las revisiones anteriores;
- Las actualizaciones o cambios en la tecnología, normatividad y procesos aplicables e implementados;
- Los requerimientos por parte de autoridades;
- Las quejas, y
- Las vulneraciones de seguridad.

La instancia responsable del cumplimiento recae en el Comité de Transparencia y la Unidad de Transparencia.

PROGRAMA GENERAL DE CAPACITACIÓN (anexo 11).

En cumplimiento al artículo 35 fracción VII de la Ley General y artículo 50 fracción XIX de la Ley Estatal se deberá elaborar el programa anual de Capacitación.

El programa de capacitación deberá ser a corto, mediano y largo plazo y estar dirigidos a los responsables del tratamiento de datos personales y deberá contemplar lo siguiente:

- Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Principios que regulan el tratamiento de datos personales, deberes y obligaciones de los sujetos responsables.
- Inventario de Datos Personales.
- Medidas de seguridad orientadas a la protección de datos personales.
- Las amenazas, valoración y vulneraciones a los datos personales.
- Causas de sanción por incumplimiento de las obligaciones establecidas la ley.

El programa anual de capacitación estará coordinado por el Instituto de Formación, Profesionalización y Carrera Judicial.

PROGRAMA DE CAPACITACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES 2023

No.	N O R M A T I V A	T E M A R I O	PONENTES / INSTRUCTORES	CALENDARIO
01	DISPOSICIONES CONSTITUCIONALES (DERECHO A LA PROTECCIÓN DE DATOS PERSONALES)	Ponencia	Presidente del Comité de Transparencia (Ponente)	ENERO 2023
02	LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS	Ponencia	Directora de Transparencia y Acceso a la Información Pública (Ponente)	ENERO 2023
03	LINEAMIENTOS GENERALES DE PROTECCIÓN DE DATOS PERSONALES PARA EL SECTOR PÚBLICO	Ponencia	Directora de Transparencia y Acceso a la Información Pública (Ponente)	ENERO 2023
04	LOS PRINCIPIOS Y DEBERES DE LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES	Ponencia	Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas (Ponente)	ENERO 2023
05	LOS DERECHOS ARCO	Acceso, Rectificación, Cancelación y Oposición de los Datos Personales	Directora del Archivo Judicial (Instructora)	FEBRERO 2023
06	EL AVISO DE PRIVACIDAD	Aviso de Privacidad Integral y Simplificado	Directora de Transparencia y Acceso a la Información Pública (Instructora)	FEBRERO 2023
07	SISTEMA Y DOCUMENTO DE SEGURIDAD DE LOS DATOS PERSONALES	El inventario de datos personales y de los sistemas de tratamiento	Directora de Transparencia y Acceso a la Información Pública (Instructora)	FEBRERO 2023
		Las funciones y obligaciones de las personas que traten datos personales	Directora de Transparencia y Acceso a la Información Pública (Instructora)	FEBRERO 2023
		Las medidas de seguridad de datos personales	Directora de Transparencia y Acceso a la Información Pública (Instructora)	MARZO 2023
		El análisis de riesgos de los datos personales	Directora de Transparencia y Acceso a la Información Pública (Instructora)	MARZO 2023
		Los niveles de riesgo de los datos personales	Directora de Transparencia y Acceso a la Información Pública (Instructora)	MARZO 2023
		El análisis de brecha, medidas de seguridad faltantes	Directora de Transparencia y Acceso a la Información Pública (Instructora)	MARZO 2023
		El Plan de trabajo para la implementación de las medidas de seguridad faltantes	Directora de Transparencia y Acceso a la Información Pública (Instructora)	MARZO 2023
08	LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD	Ponencias	Contralor Interno y Directora de Transparencia y Acceso a la Información Pública (Ponentes)	ABRIL 2023
09	DE LAS MEDIDAS DE APREMIO	Ponencia	Contralor Interno (Ponente)	ABRIL 2023

ELABORÓ

LIC. BLANCA ESTHELA COUTIÑO SÁNCHEZ
DIRECTORA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

AUTORIZÓ

LIC. LUIS ALFREDO SIERRA SÁNCHEZ
PRESIDENTE DEL COMITÉ DE TRANSPARENCIA

DE LAS MEDIDAS DE APREMIO

A continuación, por su importancia se reproduce íntegramente las medidas de apremio establecidas por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

Artículo 179.- El Instituto podrá imponer las siguientes medidas de apremio para asegurar el cumplimiento de sus determinaciones:

I. La amonestación pública, o

II. La multa, equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la unidad de medida y actualización.

El incumplimiento de los responsables será difundido en el Portal de Obligaciones de Transparencia del Instituto y considerado en las evaluaciones que realicen éstos.

Artículo 180.- Para calificar las medidas de apremio establecidas en el presente Capítulo, el Instituto deberá considerar:

I. La gravedad de la falta del responsable, determinada por elementos tales como el daño causado; los indicios de intencionalidad; la duración del incumplimiento de las determinaciones del Instituto y la afectación al ejercicio de sus atribuciones.

II. La condición económica del infractor.

III. La reincidencia.

El Instituto deberá establecer mediante lineamientos de carácter general, las atribuciones de las áreas encargadas de calificar la gravedad de la falta de observancia a sus determinaciones y de la notificación y ejecución de las medidas de apremio que se apliquen e implementen, conforme a los elementos desarrollados en este Capítulo.

Artículo 181.- El Instituto podrá requerir al infractor la información necesaria para determinar su condición económica, apercibido de que en caso de no proporcionar la misma, las multas se cuantificarán con base en los elementos que se tengan a disposición, entendidos como los que se encuentren en los registros públicos, los que contengan medios de información o sus propias páginas de Internet y, en general, cualquiera que evidencie su condición, quedando facultado el Instituto para requerir aquella documentación que se considere indispensable para tal efecto a las autoridades competentes.

Artículo 182.- En caso de reincidencia, el Instituto podrá imponer una multa equivalente hasta el doble de la que se hubiera determinado.

Para efectos de la presente Ley, se considerará reincidente al que habiendo incurrido en una infracción que haya sido sancionada, cometa otra del mismo tipo o naturaleza.

Artículo 183.- Las medidas de apremio a que se refiere el presente Capítulo, deberán ser aplicadas por el Instituto por sí mismo o con el apoyo de la autoridad competente, de conformidad con los procedimientos que establezcan las leyes respectivas.

Artículo 184.- Las multas que fije el Instituto se harán efectivas ante la Secretaría de Hacienda del Gobierno del Estado de Chiapas, a través de los procedimientos que las leyes establezcan y el mecanismo implementado para ello.

Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos.

Artículo 185.- Las medidas de apremio deberán aplicarse e implementarse en un plazo máximo de quince días, contados a partir de que sea notificada la medida de apremio al infractor.

Artículo 186.- La amonestación pública será impuesta por el Instituto y será ejecutada por el superior jerárquico inmediato del infractor con el que se relacione.

Artículo 187.- Si a pesar de la ejecución de las medidas de apremio previstas en el presente Capítulo no se cumpliere con la resolución, se requerirá el cumplimiento al superior jerárquico para que en el plazo de cinco días lo obligue a cumplir sin demora. De persistir el incumplimiento, se aplicarán sobre aquél las medidas de apremio a que se refiere el artículo 183 de la presente Ley.

Transcurrido el plazo, sin que se haya dado cumplimiento, se dará vista a la autoridad competente en materia de responsabilidades.

Artículo 188.- En contra de la imposición de medidas de apremio, procede el recurso correspondiente ante el Poder Judicial del Estado de Chiapas, y en su caso, el juicio de amparo ante el Poder Judicial de la Federación.

Artículo 189.- En caso que del contenido de las actuaciones y constancias de los procedimientos ventilados ante el Instituto, se advierta la presunta comisión de delitos y éstos se persigan de oficio, se deberá dar el aviso correspondiente al Fiscal del Ministerio Público, remitiéndole copia de las constancias conducentes.

Artículo 190.- En caso de que el incumplimiento de las determinaciones del Instituto implique la presunta comisión de un delito, éste deberá denunciar los hechos ante la autoridad competente.

DE LAS RESPONSABILIDADES ADMINISTRATIVAS Y SUS SANCIONES

Artículo 191.- Serán causas de responsabilidad administrativa por incumplimiento de las obligaciones establecidas en la presente Ley, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO o de la portabilidad de los datos personales.

II. Incumplir los plazos de atención previstos en la presente Ley, para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate.

III. Ampliar con dolo los plazos previstos en la presente Ley, para responder las solicitudes para el ejercicio de los derechos ARCO o la portabilidad de los datos personales.

IV. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.

V. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley.

VI. Mantener los datos personales inexactos cuando resulte imputable al responsable.

VII. No efectuar la rectificación, cancelación u oposición al tratamiento de los datos personales que legalmente proceda, cuando resulten afectados los derechos de los titulares.

VIII. No contar con el aviso de privacidad ya sea simplificado o integral, o bien, omitir en el mismo alguno de los elementos a que refieren los artículos de la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia.

IX. Clasificar, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en la Ley de Transparencia. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales.

X. Incumplir el deber de confidencialidad establecido en el artículo 57 de la presente Ley.

Xl. No establecer las medidas de seguridad en los términos que establecen los artículos 47, 48 y demás aplicables de la presente Ley.

XII. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad.

XIII. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley.

XIV. Obstruir los actos de verificación de la autoridad.

XV. Crear bases de datos personales en contravención a lo dispuesto por el artículo de la presente Ley.

XVI. No acatar las resoluciones emitidas por el Instituto.

XVII. Aplicar medidas compensatorias en contravención de los criterios que tales fines establezca el Sistema Nacional.

XVIII. Declarar dolosamente la inexistencia de datos personales cuando éstos existan total o parcialmente en los archivos del responsable.

XIX. No atender las medidas cautelares establecidas por el Instituto.

XX. Tratar los datos personales de manera que afecte o impida el ejercicio de los derechos fundamentales, previstos en la Constitución Política de los Estados Unidos Mexicanos.

XXI. No cumplir con las disposiciones previstas en los artículos 86, 87, 92 y demás aplicables de la presente ley, respecto de la formalización de la relación responsable y encargado y cómputo en la nube.

XXII. No presentar ante el Instituto la evaluación de impacto a la protección de datos personales en aquellos casos en que resulte obligatoria, de conformidad con lo previsto en la presente Ley y demás normativa aplicable.

XXIII. Realizar actos para intimidar o inhibir a los titulares en el ejercicio de los derechos ARCO.

XXIV. Omitir la entrega del informe anual a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo día de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, XV, XVI, XVIII, XIX y XX, del presente artículo, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.

LAS SANCIONES DE CARÁCTER ECONÓMICO NO PODRÁN SER CUBIERTAS CON RECURSOS PÚBLICOS.

Artículo 192.- Ante incumplimientos por parte de los partidos políticos, el Instituto dará vista, según corresponda, al Instituto Nacional Electoral o al Instituto de Elecciones y Participación Ciudadana del Estado de Chiapas, para que investigue, resuelva y, en su caso, sancione lo conducente, sin perjuicio de las sanciones establecidas para los partidos políticos en las leyes aplicables.

Artículo 193.- En el caso de probables infracciones relacionadas con fideicomisos o fondos públicos, el Instituto deberá dar vista al órgano interno de control o instancia equivalente del responsable relacionado con éstos, cuando sean servidores públicos, con el fin de que instrumenten los procedimientos administrativos a que haya lugar.

Artículo 194.- En aquellos casos en que el presunto infractor tenga la calidad de servidor público, el Instituto deberá:

I. Elaborar una denuncia dirigida al órgano interno de control o instancia equivalente, con la descripción precisa de los actos u omisiones que, a su consideración, repercuten en la adecuada aplicación de la presente Ley y que pudieran constituir una posible responsabilidad.

II. Remitir un expediente que contenga todos los elementos de prueba que considere pertinentes para sustentar la presunta responsabilidad administrativa. Para tal efecto, deberá acreditar el nexo causal existente entre los hechos controvertidos y las pruebas presentadas.

La denuncia y el expediente respectivo deberán remitirse al órgano interno de control o instancia equivalente dentro de los quince días siguientes, a partir de que el Instituto tenga conocimiento de los hechos.

La autoridad que conozca del asunto, deberá informar de la conclusión del procedimiento y en su caso, de la ejecución de la sanción al Instituto.

Artículo 195.- Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto por el artículo 191 de la presente Ley, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

Para tales efectos, el Instituto podrá denunciar ante las autoridades competentes cualquier acto u omisión violatoria de la presente Ley y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.

BIBLIOGRAFÍA CONSULTADA

Metodología de Análisis de Riesgo BAA (Beneficio para el atacante, la Accesibilidad para el atacante y la Anonimidad del atacante), versión de marzo 2014, publicado por el IFAI.

Metodología de Análisis de Riesgo BAA (Beneficio para el atacante, la Accesibilidad para el atacante y la Anonimidad del atacante), versión de junio 2015, publicado por el IFAI.

Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, versión de junio 2015, publicada por el INAI.

Guía para el Borrado Seguro de Datos Personales, versión de junio de 2016, publicada por el INAI.

Guía para la Protección de Datos Personales con Perspectiva de Gestión Documental y Archivos, versión mayo de 2021, publicada por el INAI.

Guía para la elaboración de un Documento de Seguridad versión 1.4 de agosto de 2016 publicada por el INAI.

Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas versión de junio 2014, publicado por el IFAI.

Medidas de seguridad en los datos personales. Versión de 2015 publicada por el INAI.

Recomendaciones para el manejo de incidentes de seguridad de datos personales – publicada por el INAI, Edición junio 2018.

Guía para la protección de datos personales con perspectiva de gestión documental y archivos - Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales - Edición, mayo de 2021.

Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración respecto al riesgo, edición de abril 2021, publicado por el INAI.

Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales, publicado por el INAI.

Programa de Protección de Datos, Documento Orientador, (INAI, versión agosto de 2018).

Recomendaciones para los Sujetos Obligados en la designación del oficial de datos personales, publicado por el INAI.

Medidas de Seguridad “Deber de Seguridad”, Documento de Seguridad, Anexo 6, (INAI)

Documento Orientador para la elaboración del Programa de Protección de Datos, versión de agosto de 2018, elaborado por el INAI.

Guía para la integración del documento de seguridad elaborado por el Comité de Transparencia del Consejo de la Judicatura Federal.

Guía práctica para elaborar un documento de seguridad. - Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco.

Documento de seguridad para Sistemas de Datos Personales en medios físicos del H. Ayuntamiento de Villa Guerrero, Jalisco.

Manual en materia de Seguridad de Datos Personales, del Instituto Nacional Electoral.

Catálogo de Datos Personales, Criterios y Resoluciones para su Tratamiento, elaborado por la Unidad de Transparencia de la SEMARNAT, actualización del 14 de noviembre de 2018.

E L A B O R A C I O N	A P R O B A C I O N
JORGE LUIS GORDILLO ZEPEDA **RESPONSABLE DEL ÁREA DE PROTECCIÓN DE DATOS**	**LIC. BLANCA ESTHELA COUTIÑO SÁNCHEZ** **DIRECTORA DE LA UNIDAD DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA**