idaip
Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo

Documento de seguridad para la protección de datos personales

Comité de Transparencia
02 de agosto de 2023

Por tu derecho a saber

GLOSARIO

Bases de Datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados que permitan su tratamiento, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento u organización.

Ciclo de vida: Tiempo que duración y conclusión del tratamiento de los datos personales, para después ser suprimidos, cancelados o destruidos por parte del responsable.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas.

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. Se consideran sensibles de manera enunciativa más no limitativa, los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas, datos biométricos, preferencia sexual y de género;

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad de carácter técnico, físico y administrativo adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Finalidad: Los datos personales recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados. Los datos personales con fines de archivo, de interés público, investigación científica e histórica, o estadísticos no se considerarán incompatibles con la finalidad inicial.

Instituto: Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo.

Ley de datos: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan garantizar la confidencialidad, disponibilidad e integridad de los datos personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad a nivel organizacional, identificación, clasificación y borrado seguro de los datos personales, 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 del responsable sus instalaciones físicas, áreas críticas, recurso y datos personales.

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización del responsable, recursos y datos personales.
c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización del responsable.
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 personales, 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.
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Responsable: Cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Partidos Políticos, Fideicomisos y Fondos Públicos, que decida y determine finalidad, fines, medios, medidas de seguridad y demás cuestiones relacionadas con el tratamiento de datos personales.

Sistema de datos personales: Conjunto de organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de los sujetos obligados, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Los sistemas de datos personales se distinguen en:

Físicos: Conjunto ordenado de datos de carácter personal que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos, estructurado conforme a criterios específicos relativos a personas físicas que permitan acceder sin esfuerzos desproporcionados a sus datos personales.

Automatizados: Conjunto ordenado de datos de carácter personal que permita acceder a la información relativa a una persona física utilizando una herramienta tecnológica.

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

Soporte físico: 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, demás análogos.

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

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionados de manera enunciativa más no limitativa con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia y en general cualquier uso o disposición de datos personales.

Unidad de Transparencia: Instancia que auxilia, orienta, gestiona, establece, informa, propone, aplica, asesora, registra y realiza las gestiones necesarias para el manejo, mantenimiento, seguridad, y protección de los sistemas de datos personales en posesión del responsable.

Usuario: Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas de datos personales.

Vulneración de datos personales: Es la materialización de las amenazas pudiendo estar enfocadas a la pérdida o destrucción no autorizada de los datos personales, el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, así como el daño, alteración o modificación no autorizada.

INTRODUCCIÓN

El Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo en adelante IDAIPQROO, reconoce el Derecho Humano de la protección de datos personales, establecido en la Constitución Política de los Estados Unidos Mexicanos en los artículos 6, apartado A, fracciones II y III y 16, segundo párrafo.

A partir de la reforma constitucional de 2009, la protección de datos personales quedó establecida como un derecho fundamental, el cual reconoce que toda persona tiene derecho a la protección, y al ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de sus datos personales.

El 26 de enero de 2017 se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en lo sucesivo, la Ley General), que tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de los sujetos obligados.

En fecha 04 de julio de 2017, se publicó la **Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo** reformada el 18 de Enero de 2018; de observancia obligatoria en todo el territorio del Estado de Quintana Roo y sus Municipios, que tiene por objeto garantizar el derecho que tiene

toda persona a la protección de sus datos personales, en posesión de los Responsables.

El 26 de enero de 2018, se publicó en el Diario Oficial de la Federación los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) cuyo objetivo es desarrollar las disposiciones previstas en la Ley General y, con ello, hacer más comprensible el cumplimiento de los principios, deberes y obligaciones exigidos en materia de protección de datos personales.

En este sentido, el **IDAIPQROO**, reconoce la necesidad de observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, responsabilidad; así como los deberes de seguridad y confidencialidad que derivan de las Leyes en materia de datos personales.

Dichos principios y deberes dictan una serie de obligaciones de observancia para los responsables, que tiene como propósito que el tratamiento se realice garantizando la protección de los datos personales de sus titulares.

En relación con el deber de seguridad, los responsables deben elaborar un Documento en el que se establezcan las medidas de seguridad de carácter administrativo, físico y técnico que han de adoptar para el adecuado tratamiento de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado a través del ciclo de vida de los datos personales; así como garantizar su confidencialidad, integridad y disponibilidad.

OBJETIVO DEL DOCUMENTO DE SEGURIDAD

Garantizar que todo tratamiento de datos personales cuente con las medidas de seguridad necesarias para la protección de los mismos y el cumplimiento de las obligaciones previstas en la Ley de datos.

De conformidad con el artículo 34 de la Ley de datos, establece que el responsable debe realizar las siguientes actividades interrelacionadas:

- Crear Políticas internas para la gestión y tratamiento de los datos.
- Establecer de acuerdo al marco normativo, las funciones y obligaciones de las unidades administrativas que son responsables del uso y manejo de datos personales.
- Realizar un inventario de datos personales y de los sistemas de tratamiento.
- Realizar un análisis de riesgo, de brecha y elaborar un Plan de Trabajo.
- Monitorear y revisar de manera periódica las medias de seguridad implementadas.
- Realizar capacitaciones a efecto de que el personal del instituto cuente con las herramientas que permitan el correcto

tratamiento de los datos personales, acordé a su ámbito de responsabilidad.

RESPONSABILIDADES

En apego al artículo 95 de la Ley de datos, establece que el responsable en materia de protección de datos personales, es el Comité de Transparencia.

Es así que cada Sujeto Obligado contará con un Comité, el cual se integrará y funcionará conforme los establece la Ley de Transparencia y Acceso a la Información Pública para el Estado de Quintana Roo y demás normatividad aplicable.

Dicho Órgano, tendrá dentro de sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales. En esa tesitura dicho órgano tiene las funciones siguientes:

I. Aprobar, supervisar y evaluar las políticas, programas, acciones, en conjunto con las áreas técnicas que estime necesario, involucrar o consultar;

II. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en el ámbito de organización del responsable, que resulten

aplicables en la materia, en coordinación con el oficial de protección de datos personales, en su caso;

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

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

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

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

VII. Dar seguimiento y cumplimiento a las resoluciones emitidas por el instituto nacional.

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

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

Las unidades administrativas deberán realizar las acciones necesarias para cumplir con las obligaciones que establece este documento, para lo cual, deberán asignar los recursos materiales y humanos necesarios, y prever lo que se requiera en sus programas de trabajo.

I. POLITICAS INTERNAS

El Sistema de Gestión de Datos Personales es el medio por el cual el **Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Quintana Roo**, garantiza el tratamiento de los datos personales que lleva a cabo como parte de sus funciones, desde su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación correspondiente; para lo cual, se establecen políticas y métodos orientados a salvaguardar la confidencialidad, integridad y disponibilidad de estos datos, de acuerdo con Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo.

II. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

Es un control documentado que permite identificar los procesos en los que las unidades administrativas del Instituto tratan datos personales.

Es a través de esas bases de datos en las que se documenta la información básica de cada tratamiento, con independencia de su forma de almacenamiento.

En el Instituto se cuenta con 12 áreas que tratan datos personales

Las personas encargadas de llevar a cabo el tratamiento de datos, tienen como funciones y obligaciones las siguientes:

- Garantizar la seguridad en el tratamiento de datos personales, esto con la finalidad de evitar algún riesgo, como la pérdida, robo, alteración o acceso no autorizado.
- Garantizar la debida protección de los datos personales, conforme a la Ley de datos y las demás disposiciones aplicables en la materia.
- Implementar medidas de seguridad físicas, técnicas y administrativas convenientes para el tratamiento diario de los datos personales.
- Garantizar la confidencialidad de los datos personales derivada de los procedimientos que tienen a su cargo.
- Conocer y aplicar las acciones derivadas de este Documento de Seguridad.
- Garantizar el cumplimiento de los derechos ARCO a los titulares de los datos personales.

1. **Secretaría Ejecutiva**

1.1. Expedientes de Recursos de Revisión en materia de derecho de acceso a la información.

1.2. Expedientes de Recursos de Revisión en materia de

protección de datos personales.

2. Coordinación de Capacitación.

2.1. Registro a Eventos de Capacitación Presencial del IDAIPQROO a los Sujetos Obligados.

2.2. Concurso infantil de dibujo del IDAIPQROO 2019 Edición 13

2.3. Sistema para el Proceso de Certificación de Unidades de Transparencia (Siproce)

2.4. Sistema de Capacitación (SICAP) del IDAIPQROO

2.5. Formulario de Registro a Cursos y Talleres en línea del IDAIPQROO.

2.6. Directorio de Enlace de Capacitación de la Red Local del Estado de Quintana Roo.

2.7. Cuestionario de Detección de Necesidades de Capacitación de los Trabajadores del IDAIPQROO.

2.8. Concurso infantil de dibujo del IDAIPQROO 2021 Edición 14

2.9. Registros a eventos de capacitación presencial en el sector educativo: nivel medio superior y superior.

2.10. Registro a las acciones de capacitación del IDAIPQROO a estudiantes de nivel básico.

2.11. Concurso infantil de dibujo del IDAIPQROO 2022 Edición

2.12. Diplomado en Transparencia, Acceso a la información y Protección de Datos Personales

3. Coordinación Jurídica y de Datos Personales

3.1. Expedientes de Recursos de Revisión en materia de derecho de acceso a la información.

3.2. Expedientes de Recursos de Revisión en materia de protección de datos personales.

4. Coordinación de Vinculación

4.1. Denuncia por incumplimiento de obligaciones de transparencia.

4.2. Seguimiento a las resoluciones emitidas por incumplimiento de obligaciones de trasparencia

4.3. Directorio de titulares de unidades de transparencia de los sujetos obligados del Estado.

5. Unidad de Transparencia

5.1. Sistema de Solicitudes de Acceso a la Información (SAI).

5.2. Sistema de solicitudes de Derecho ARCO.

6. Órgano Interno de Control

6.1. Presentación de Declaración de situación Patrimonial y de Intereses.

6.2. Quejas, denuncias y sugerencias.

7. Dirección de Recursos Humanos, Materiales y Servicios Generales

7.1. Expediente de personal.

7.2. Registro de asistencia.

7.3. Prestadores de servicio social y prácticas profesionales del IDAIPQROO.

7.4. Expediente de proveedores.

8. Dirección de Comunicación Social

8.1. Directorio de Periodistas y personas vinculadas a prensa y medios de comunicación.

8.2. Archivo de imágenes y fotografías para la difusión institucional.

9. Dirección de Protección de Datos Personales

9.1. Expedientes de denuncias de datos personales (procedimiento de vigilancia y verificación de tratamientos de datos personales)

10. Dirección de Tecnologías de la Información

10.1. Registro de Usuarios del sistema INFOMEX.

10.2. Videos de Vigilancia.

11. Subdirección Administrativa

11.1. Registro de entradas y salidas a las instalaciones del

IDAIPQROO.

12. Gestión Documental

12.1. Directorio de Enlaces de Archivo del Estado de Quintana Roo.

Con la información recabada a través el inventario de datos personales, se pudo percibir la importancia de analizar cada uno de los principios que señala la Ley de datos; y en consecuencia acorde a cada sistema de tratamiento, se realizaron las actualizaciones de

los avisos de privacidad; cabe resaltar que en el art. 19 de la Ley de datos, señala cuando el responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales.

III. LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES

De conformidad a los artículos 34 Fracción II y 37 Fracción II de la Ley de datos, se describen las funciones y Obligaciones del personal involucrado en el tratamiento de datos personales, en apego a las facultades establecidas en el Reglamento Interior y Condiciones Generales de Trabajo del Instituto de Acceso a la Información y Protección de Datos Personales.

IV. ANÁLISIS DE RIESGOS, ANÁLISIS DE BRECHA Y PLAN DE TRABAJO

En apego al art. 34 fracción IV, el análisis de riesgo debe ser elaborado considerando las amenazas y vulnerabilidades existentes, identificando los riesgos latentes respecto de cada uno de los tratamientos de datos personales.

Atendiendo lo anterior las áreas que tratan datos personales, realizaron un análisis, acorde a cada sistema en base a lo siguiente:

Análisis de Riesgos

El análisis de riesgos es un **proceso sistemático** para conocer y determinar la **magnitud de los riesgos** a los que se encuentran expuestos los **activos** de responsable. El análisis de riesgos permite determinar cómo es, cuánto vale y cómo está protegido cada activo (identificando posibles problemas), y anticiparse a las futuras dificultades, lo que nos permitirá tomar mejores decisiones y actuar con oportunidad.

En el análisis de riesgos deben considerarse los siguientes elementos:

- **Activos**, que se dividen en dos tipos:
  - Activos de información: Datos personales;
  - Activos de apoyo: Elementos físicos e infraestructura que soportan los activos de información;
- **Amenazas**: Eventos con la capacidad de causar daño a una organización;
- **Vulnerabilidades**: Debilidades de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

Metodología BAA

Se enfoca en tres variables que afectan la percepción del valor de los datos personales para un atacante:

- Beneficio para el atacante;
- Accesibilidad para el atacante;
- Anonimidad del atacante.

Identificación y clasificación de datos personales

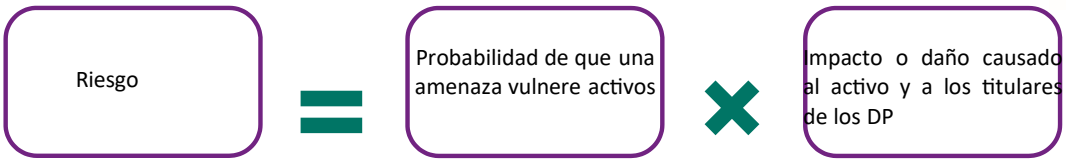
- Clasificación de datos personales;
- Identificación de tipos de datos y de nivel de riesgo inherente.

Análisis de riesgos de datos personales

- Identificación de riesgo por tipo de dato;
- Identificación del nivel de riesgo por tipo de dato;
- Cuestionario de autoevaluación;
- Identificación de nivel de accesibilidad;
- Identificación de nivel de anonimidad;
- Identificación de nivel de riesgo latente.

Identificación de medidas de seguridad

- Tablas de control;
- Procedimiento de selección de medidas de seguridad.



Derivado del análisis del formato proporcionado, es posible identificar:

1. **Tipo de dato que se trata. (Volumen de titulares que conforman la base de datos.)**

TIPO DE DATO	RIESGO INHERENTE	NIVEL DE RIESGO
Datos identificativos	Bajo	1
Datos electrónicos; laborales; patrimoniales; procedimientos administrativos	Medio	2
Datos de tránsito y movimientos migratorios; sobre la salud; biométricos.	Alto	3
Datos especialmente protegidos (sensibles).	Muy alto	4-5

NIVEL DE RIESGO POR TIPO DE DATO Tipo de dato/número de titulares	>100	>1000	>10,000	<10,000
Datos identificativos	1	1	1	1
Datos electrónicos; laborales; patrimoniales; procedimientos administrativos	1	1	2	2
Datos de tránsito y movimientos migratorios; sobre la salud; biométricos.	1	2	3	3
Datos especialmente protegidos (sensibles).	4	4	5	5

2. **Riesgo por tipo de acceso.**

3. **Riesgo por entorno.**

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

La combinación de los tres factores analizados permitió definir el nivel de riesgo latente por tratamiento, lo cual contribuirá a identificar el nivel de medidas de seguridad que deban implementarse en cada caso.

Análisis de Brecha

Consistente en identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados, cuya información da sustento a las políticas y mecanismos institucionales en materia de protección de datos personales que se deban aprobar. Lo anterior con el objetivo de atenderlas de manera escalonada y en coordinación con cada una de las áreas.

Derivado del análisis fue posible identificar como vulneraciones comunes:

1. Robo de información, modificación-destrucción no autorizada de la información, acceso no autorizado a los sistemas.
2. Daños estructurales, fuego, inundación.
3. Fenómenos climáticos y sísmicos.

V. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Cuando hablamos de los mecanismos de monitoreo y revisión de las medidas de seguridad en protección de datos personales, nos referimos a todas las acciones, actividades, instrumentos, herramientas, controles o mecanismos administrativos, técnicos y físicos que permitan protegerlos contra daño, pérdida, alteración, destrucción, uso o acceso no autorizado, garantizando con ello la confidencialidad, integridad y disponibilidad de los datos personales.

Con la finalidad de identificar las medidas de seguridad de manera enunciativa se describen las medidas comunes.

1. **Medidas de seguridad administrativas**: Acciones y mecanismos implementados en el tratamiento de datos personales a nivel organizacional, como lo son las políticas y procedimientos para la gestión y revisión de la seguridad de la información, identificación, clasificación y borrado seguro de la información, así como sensibilización y capacitación del personal, en materia de protección de datos personales.

2. **Medidas de seguridad físicas:** Acciones y mecanismos para proteger el entorno físico, instalaciones, equipos, soportes o sistemas e datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor.

   - Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
   - Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
   - Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; y,
   - Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

3. **Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología y los recursos involucrados en su tratamiento.

- Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y
- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

VI. EL PROGRAMA GENERAL DE CAPACITACIÓN

El programa concentra los retos en materia de seguridad de datos personales que afrontan las instancias, es así que el personal del Instituto deberá capacitarse cuando menos una vez al año, con la intención de que todos los servidores públicos puedan participar.

La importancia de implementar un Sistema de Gestión de Seguridad de Datos Personales en el sector público radica en la protección de los datos personales, los cuales deben ser tratados atendiendo los principios y deberes establecidos por la Ley de datos, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de los titulares.

La correcta implementación del Sistema y constante actualización, ayuda a mitigar los efectos de una vulneración de datos personales, evita sanciones a servidores públicos responsables en el tratamiento de los datos personales, genera confianza de los titulares hacia el responsable del tratamiento, permite una constante mejora.

VII.ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

Dentro de los mecanismos se cuenta con el propósito de tener una mejora continua, actuar, planificar, verificar y hacer.

Es así que el presente documento de seguridad se actualizará cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad, e
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad; y
V. Cuando surjan documentos, formatos, recomendaciones, etc. por parte del INAI para la mejora del documento de seguridad.

idaip

Instituto de Acceso a la Información y
Protección de Datos Personales de Quintana Roo

Por tu derecho a saber

IDAIPQROO

Av. Othón P. Blanco No. 66 entre Cozumel y Josefa Ortiz de Domínguez,
Col. Barrio Bravo, Chetumal, Quintana Roo, C.P. 77098
Tel. 983 8323561