DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LA STyPS.

Contenido

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.

STyPS: Secretaría del Trabajo y Previsión Social.

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.

Sistema de Gestión de Seguridad de Datos Personales (SGSDP): Sistema de gestión 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 General, los Lineamientos Generales, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.

INTRODUCCIÓN

La Secretaría del Trabajo y Previsión Social en adelante STyPS, 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 20 de marzo de 2025 se publicó la nueva 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, la Secretaría del Trabajo y Previsión Social, 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.

UNIDADES ADMINISTRATIVAS QUE CONFORMAN LA SECRETARIA DEL TRABAJO Y PREVISIÓN SOCIAL

- ✓ Junta Local Conciliación y Arbitraje.
- ✓ Juntas Especiales de Conciliación y Arbitraje.
- ✓ Tribunal de Conciliación y Arbitraje.
- ✓ Procuraduría de la Defensa del Trabajo.
- ✓ Procuradurías Auxiliares de la Defensa del Trabajo.
- ✓ Dirección del Trabajo y Previsión Social.
- ✓ Dirección Administrativa
- ✓ Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales y Archivo.
- ✓ Dirección Jurídica y Mejora Regulatoria.

Planeación y Diagnóstico

MARCO NORMATIVO APLICABLE

Constitución Política de los Estados Unidos Mexicanos. (CPEUM).

Ley General de Transparencia y Acceso a la Información Pública. (LGTAIP).

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. (LGPDPPSO).

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el estado de Quintana Roo.

Ley de Transparencia y Acceso a la Información Pública para el estado de Quintana Roo.

Reglamento Interior de la Secretaría del Trabajo y Previsión Social.

Decreto 081 de Creación de la STYPS.

Manual de Organización de la STYPS.

Manual de Procedimientos de Trámites y Servicios de la STYPS.

ÁMBITO DE APLICACIÓN

El presente documento de seguridad constituye el instrumento que describe y da cuenta sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por la **Secretaría del Trabajo y Previsión Social (STyPS)** para garantizar el cumplimiento de los principios y deberes establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Asimismo, dicho documento será de observancia obligatoria para todos los servidores(as) públicos(as) que intervienen en el tratamiento de datos personales que se encuentren en posesión de esta secretaria, así como para toda aquella persona física o moral, pública o privada, que debido a la prestación de un servicio tenga acceso a los datos personales de conformidad con lo establecido en la LGPDPPSO.

En este sentido, la **Unidad de Transparencia, Acceso a la Información Pública, Datos Personales y Archivo** integra el presente documento de seguridad con base en la información generada por las unidades administrativas del Sujeto Obligado (STyPS) acorde al ámbito de sus funciones y, de conformidad con las disposiciones aplicables.

OBJETIVO

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.

X. 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.

DOCUMENTO DE SEGURIDAD

Artículo 35. De manera particular, el responsable deberá elaborar un documento de seguridad que

contenga, al menos, lo siguiente:

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

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

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.

ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD

¿Cómo se elaboró el Documento de Seguridad?

De conformidad con el artículo 15 del Acuerdo General, el Documento de Seguridad debe ser elaborado por la Unidad de Transparencia con la información que cada una de las instancias de la Secretaría del Trabajo y Previsión Social proporcionen.

En atención a ello, para constituir el presente instrumento se siguió la metodología siguiente:

1. Se formuló la Guía para la integración del documento de seguridad a través de la cual se proporcionó a las instancias que realizan el tratamiento de datos personales las nociones del derecho a la protección de datos personales y los deberes de las instancias de la Secretaria del Trabajo y

Previsión Social, así como los pasos a seguir para la realización del listado de funciones y obligaciones de los servidores públicos involucrados, inventario de datos, análisis de riesgo, análisis de brecha y plan de trabajo. Requiriéndoles la concentración de las funciones y obligaciones de las personas servidoras públicas que intervienen en cada uno de los tratamientos que realizan, así como su respectivo inventario de los datos personales y sistemas, análisis de riesgo y de brecha y plan de trabajo.

2. Desahogado lo anterior, se integró por cada instancia el Inventario de Datos Personales y Sistemas, las Funciones y Obligaciones, el Análisis de Riesgo, el Análisis de Brecha y el Plan de Trabajo respectivo.

3. Una vez que se analizó la información obtenida, se formularon los mecanismos siguientes:

- ✓ Monitoreo y Supervisión en la Protección de los Datos Personales.
- ✓ Actuación ante Alertas y Vulneraciones a la Seguridad de los Datos Personales.
- ✓ De Auditoría en Materia de Datos Personales.

Asimismo, se creó un programa de capacitación en materia de protección de datos personales.

4. Todo lo anterior, fue integrado y sometido a consideración del Comité de Transparencia de la Secretaría del Trabajo y Previsión Social, órgano que aprobó el Documento de Seguridad en su Tercera Sesión Ordinaria celebrada el 23 de Octubre de 2025.

Cabe indicar que de conformidad con el artículo 83, segundo párrafo y 84, fracciones I, V y VII, de la Ley General, el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales, contando con las atribuciones de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales; supervisar, en coordinación con las instancias competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad; así como establecer programas de capacitación y actualización para las personas servidoras públicas en materia de protección de datos personales.

En la Tercera Sesión Ordinaria celebrada el 23 de Octubre 2025, el Comité de Transparencia aprobó la creación del Documento de Seguridad.

Relación de Datos Personales de la Dirección del Trabajo y Previsión Social

1. El nombre del patrón o representante legal de la empresa.
2. El nombre del Secretario del Sindicato o representante legal del mismo y a
3. falta de estos un representante común de los trabajadores, debidamente
4. acreditado.
5. El nombre de dos testigos de asistencia con identificación propuestos por la
6. parte patronal (en caso de negativa a proporcionarlos el inspector designará).
7. Acta Constitutiva de la persona moral (fuente de trabajo).
8. Actividad o giro comercial.
9. Registro Federal de Contribuyentes.
10. Registro Patronal ante el Instituto Mexicano de Seguro Social (IMSS).
11. Organismo empresarial al que pertenece.
12. En caso de tener Contrato Colectivo nombre del Sindicato y/o Central Obrera.
13. Domicilio fiscal.
14. Nombres de los integrantes de la Comisión Mixta de Capacitación,
15. Adiestramiento y Productividad.
16. Nombres de los integrantes de la Comisión Mixta de Seguridad e Higiene.
17. Reglamento Interior de Trabajo.
18. Si tiene contratado algún menor, los permisos correspondientes para laborar.
19. Nombres de las Trabajadoras en Período de Lactancia.
20. Nombre de las Mujeres trabajadoras en Estado de Gestación.
21. Reparto de utilidades (recibos de pagos que contienen nombres y numero de
22. seguridad social, RFC de la empresa).
23. Vacaciones.
24. Aguinaldo.
25. Días de descanso.
26. Jornada de trabajo.
27. Pago de Tiempo Extraordinario.
28. Monto y Plazo de Pago del Salario.
29. Tipo de Contratación.
30. Identificación oficial (Credencial para votar con fotografía, licencia de manejo,
31. pasaporte, cédula profesional).

32. Solicitud por parte de la madre o tutor donde manifiesta:
33. Tipo de trabajo.
34. Nombre completo del menor.
35. Horario laboral.
36. Firma de la madre, padreo tutor.
37. Credencial de elector del solicitante (madre, padre o tutor).
38. Acta de nacimiento del menor y de la madre, padre o tutor.
39. Constancia de estudios del menor.
40. Comprobante de domicilio.
41. Fotografías del menor.

Datos sensibles:

42. ● Datos de Salud: Certificado médico del menor.

Relación de Datos Personales de la Dirección Administrativa

1. Fecha de Nacimiento
2. Registro Federal de Contribuyentes (R.F.C.).
3. Cédula Única de Registro de Población (C.U.R.P.)
4. Sexo.
5. Edad.
6. Dirección.
7. Estado Civil.
8. Fotografías.

Datos sensibles:

9. Datos de Salud: Certificado médico.

Así como los siguientes documentos:

10. Solicitud de Empleo debidamente requisitada.
11. Acta de Nacimiento.
12. Credencial para votar con fotografía.
13. Certificado de Estudios.
14. Antecedentes No Penales.
15. Constancia de No Inhabilitación Expedida por la Contraloría.
16. Constancia de Residencia.
17. Cartas de Recomendación.
18. Cartilla Militar.
19. Currículum Vitae.
20. Título y Cédula Profesional.
21. Cédula de Inscripción al Padrón de Profesionistas

Relación de Datos Personales del Tribunal de Conciliación y Arbitraje

1. Nombre(s) y Apellidos(s).
2. Domicilio particular.
3. Ocupación.
4. Estado civil.
5. Género (masculino y femenino).
6. Edad.
7. Registro Federal de Contribuyentes (R.F.C.).
8. Clave Única de Registro de Población (CURP).
9. Datos de Identificación oficial (IFE, INE, PASAPORTE, Licencia de conducir o Cédula Profesional).

Relación de Datos Personales de la Procuraduría de la Defensa del Trabajo

1. Nombre.
2. Domicilio particular.
3. Teléfono.
4. Dirección de correo electrónico.
5. Edad.
6. Sexo.
7. Datos de Identificación oficial.

Relación de Datos personales de la Junta Local de Conciliación y Arbitraje

1. Nombre(s) y Apellidos(s).
2. Domicilio particular.
3. Ocupación.
4. Estado civil.
5. Género (masculino y femenino).
6. Edad.
7. Datos de Identificación oficial (IFE, INE, PASAPORTE, Licencia de conducir o Cédula Profesional).
8. Número(s) de cuenta(s) bancaria(s).
9. Registro Federal de Contribuyentes.
10. Clave Única de Registro de Población.

Nombre completo del solicitante.

1. Tipo de Persona (si es trabajador o patrón)
2. Domicilio con calle, número y código postal.

3. Localidad.
4. Correo electrónico.
5. Teléfono.

Relación de Datos Personales recabados en diversas actividades de la STyPS

1. Nombre Completo
2. Correo Electrónico
3. Número de Contacto
4. Sector al que pertenece
5. Municipio
6. Localidad
7. Dependencia U Organización
8. Número Telefónico Laboral
9. Firma

FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE INTERVENGAN EN EL TRATAMIENTO DATOS PERSONALES

Todos los servidores de la Secretaría del Trabajo que tengan acceso a los datos personales, están obligados a conocer y aplicar las medidas de seguridad propias que sean de carácter administrativo, físico y técnico para la protección de datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción, o en su caso, se deberá de garantizar la confidencialidad, integridad y disponibilidad. Funciones genéricas en cualquier nivel de tratamiento:

- ✓ Tener a la vista el Aviso de Privacidad.
- ✓ Tratar los datos personales con responsabilidad y las medidas de seguridad que se haya establecido para tal fin.
- ✓ Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.
- ✓ Estar capacitado en materia de tratamiento de datos personales.
- ✓ Dar aviso a los superiores jerárquicos, ante cualquier acción que pueda poner en riesgo los datos personales, y en general que puedan vulnerar la seguridad de los datos personales.
- ✓ Conocer y seguir las medidas de seguridad que le sean aplicables para el cuidado de los datos personales, durante el periodo en el que posea los datos personales.
- ✓ Recabar los datos personales para la finalidad para la cual estos fueron solicitados según el trámite o el sistema de tratamiento que corresponda.

El incumplimiento a lo establecido en este Documento de Seguridad, así como lo establecido por la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Quintana Roo, será causa de aplicación de medidas de apremio y/o sanción de acuerdo a lo dispuesto en el artículo 171 de del mismo ordenamiento.

Una vez que se contó con la integración de los inventarios de datos, se llevó a cabo la elaboración del análisis de riesgo y brecha, atendiendo a lo previsto en el artículo 33, fracción IV y V de la Ley General de la materia, las áreas responsables de su tratamiento identificaron el valor de los datos personales de acuerdo con su categoría y el ciclo de vida; el valor de exposición de los activos involucrados en el tratamiento; las consecuencias que pueden generarse para los titulares de dichos datos.

Ilustración 1 Ciclo de Vida de los Datos Personales en la STyPS

ANÁLISIS DE RIESGO

El análisis de riesgo, además de ayudar a visualizar las medidas de seguridad administrativas, de gestión, soporte y revisión de la seguridad de la información; físicas, como lo son las acciones o mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento y, técnicas que se valen de la tecnología para proteger el entorno digital de la información, también se han registrado nuevas medidas de seguridad que deberán

desarrollarse para fortalecer algunos de los controles que actualmente son implementados.

Para analizar los riegos de los datos personales que son objeto de tratamiento, se elaboró un instrumento que, a partir de considerar su objeto y atribuciones constitucionales, clasifica los datos en tres tipos:

1. **De identificación o contacto**, que se refieren a información por la que se identifica a una persona y/o permiten su contacto como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población o la edad.

2. **Patrimoniales**, que comprenden la información que se encuentran vinculados al patrimonio de una persona como, por ejemplo, el salario, los créditos, las tarjetas de débito, los cheques o las inversiones.

3. **Sensibles**, que consideran la información concerniente a la esfera más íntima de su titular o que su uso puede dar origen a discriminación o conlleva un riesgo grave para éste como, por ejemplo, el origen étnico, el estado de salud presente o futuro, las creencias religiosas, la opinión política o la orientación sexual.

Para la determinación del riesgo sobre esa tipología de datos personales se valora la probabilidad e impacto de que, en su obtención, almacenamiento, tratamiento, transferencia o remisión, bloqueo y/o eliminación (ciclo de vida), en correspondencia con una diversidad de activos involucrados, se materialice uno o más factores que pueden causar un daño a su titular (amenaza). Para facilitar el análisis, se establecieron cuatro tipos de amenazas:

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizado.
- Pérdida o destrucción no autorizada.

En general se tiene que la Secretaría del Trabajo y Previsión Social de Quintana Roo cuenta con 9 unidades administrativas, en las que se da tratamiento de datos personales mediante 15 procesos como se visualiza a continuación:

Secretaría del Trabajo y Previsión Social Riesgos de Procesos por Unidad Administrativa	
Tipo de Dato	**Nivel de Riesgo**
Inspecciones en Materia de Condiciones Generales de Trabajo, Aguinaldos y Pago de Utilidades.	2
Permiso de Menor.	2
Solicitudes de Acceso a la Información Pública.	1
Solicitudes de Derechos Arco.	3
Video Vigilancia de la Secretaría.	1
Expediente Único de Personal.	3
Sistema de Registro de Asistencia.	1
Tramites derivados de expedientes con Sindicatos y Personales ante el Tribunal de Conciliación y Arbitraje.	2
Procedimientos relacionados con la Asesoría Jurídica Laboral.	2
Expedición de copias certificadas.	2
Asesoría, Conciliación y Representación Laboral.	2
Asistencia a Reuniones de Trabajo, Capacitaciones, Cursos, Actividades o Eventos Realizados por la Secretaría del Trabajo y Previsión Social.	2
Consultas electrónicas realizadas por la Secretaría del Trabajo y Previsión Social.	2
Certificado médico del personal.	4
Nómina .	4

Tabla 1 Riesgos por Unidad Administrativa

ANÁLISIS DE BRECHA

Una vez identificados los posibles riesgos a los que esta Secretaria se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base las medidas de seguridad reportadas por las diversas unidades administrativas, las cuales consisten en lo siguiente:

- ✓ Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general necesarios para cada trámite.
- ✓ El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones.
- ✓ Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.

- ✓ Las llaves que se tienen de cada área se encuentran en manos de servidores públicos, autorizados por cada área.
- ✓ Una vez recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio, del cual se obtuvieron los datos personales, ya sea físico o electrónico.
- ✓ Una vez recabados los datos personales, ya realizada la carpeta o expediente electrónico, o físico, y guarda está en archiveros o puesta en resguardo electrónico, tienen acceso a esta área servidores públicos del área.
- ✓ Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el servidor público guarda los mismos en carpeta electrónica, ya sea en su computadora.
- ✓ Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.

Ahora bien, a efecto de evitar la vulneración de los datos personales en posesión de esta Secretaría, considera que además de las medidas existentes, se puede reforzar la seguridad de la información con la adopción de las siguientes prácticas:

1. **Control de acceso a la información**, consistente en mantener un control sobre las personas que recaban, administran, usas, almacenan o difunden datos personales.
   Dicho control puede realizarse a través de una bitácora en la que se señale el nombre y cargo del servidor público responsable, el proceso de tratamiento de datos personales que realiza, así como las medidas de seguridad que adopta a efecto de resguardar la información.
2. **Activos del responsable**, la cual se refiere a la asignación de responsabilidades y a la clasificación de la información.
   En ese sentido, se propone que las áreas realicen un estudio pormenorizado acerca de los procesos que se vinculen con tratamiento de información confidencial, los tramos de responsabilidad de cada encargado de la información y se documenten mediante una bitácora.
3. **Seguridad física**, en este apartado se sugiere tener archiveros en buen estado y con seguridad para el resguardo de la información
   En cuanto a la información que se resguarda de manera electrónica, se recomienda la actualización de los sistemas y el mantenimiento de los equipos.
4. **Incidentes de seguridad de información.**
   En relación con este punto y derivado del diagnóstico realizado, no se ha presentado ninguna eventualidad en la cual se hayan vulnerados los datos

personales que trata la Secretaría del Trabajo y Previsión Social, no obstante, se recomienda generar programas de capacitación respecto a las acciones a realizar ante una posible incidencia y de los mecanismos de mitigación del daño.

PLAN DE TRABAJO Y MEDIDAS DE SEGURIDAD

La existencia del documento de seguridad, busca enmarcar los deberes la Secretaría del Trabajo y Previsión Social para la máxima protección de datos personales. Debido a la importancia y el contexto actual en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad de protección de datos personales.

La finalidad de este plan es plasmar de manera enunciativa, más no limitativa, las actividades la Secretaría del Trabajo y Previsión Social realizará para la aplicación del presente documento de seguridad.

Lo anterior se realizará en base a las atribuciones establecidas en el la Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Quintana Roo.

Para la ejecución del presente documento de seguridad, dentro de los 6 meses siguientes a la emisión del presente documento:

1) Se emitirá circular para difundir la emisión del presente documento, a través de la cual se remitirá copia digital del mismo a todos los correos institucionales vigentes.
2) Se comunicará a los enlaces sobre la emisión del documento de seguridad, solicitando su apoyo para la difusión interna del mismo.
3) Se buscará la participación del IDAIPQROO para una primera capacitación básica para los servidores públicos que recaban datos personales.

El Comité de Transparencia revisará de manera anual, a partir de la emisión del presente documento de seguridad:

1) Revisar lo concerniente al índice de Datos Personales y mantenerlo actualizado.
2) Actualizar las medidas de Seguridad conforme al Sistema de Protección de Datos Personales hecho para la Secretaría del Trabajo y Previsión Social.
3) Actualizar el presente plan de trabajo.

4) Se emitirá un programa anual de capacitaciones y además se promoverá que el personal de la Secretaría del Trabajo y Previsión Social se mantenga capacitado no sólo por sus áreas internas, sino también mediante su asistencia a capacitaciones otorgadas por organismos competentes en la materia.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Se debe realizar un monitoreo y revisión de la aplicación de las medidas de seguridad, para valorar las amenazas, vulnerabilidades, aplicación correcta o incorrecta, impacto y actualización. Esto con el objetivo de que las medidas de seguridad continúan siendo efectivas e idóneas para la STyPS. Realizaremos el siguiente cuadro, donde se concentran los mecanismos de monitoreo y el objetivo de cada uno de ellos:

MECANISMOS DE MONITOREO	OBJETIVOS DEL MONITOREO
Visitas a 4 áreas cada 12 meses, de las cuales serán elegidas de forma aleatoria.	Verificar de primera mano la aplicación, actualización e impacto de las medidas de seguridad aplicadas.
Solicitar reportes a los responsables de cada área generadora de información o a los responsables del sistema de datos personales o a sus administradores sobre el manejo de datos personales conforme a las medidas de seguridad.	Monitorear avances, aplicación, eventualidades y novedades respecto a la aplicación de las medidas de seguridad.

Tabla 2 Mecanismos de Monitoreo

PROGRAMA GENERAL DE CAPACITACIÓN

Se manejarán las capacitaciones de conformidad con las necesidades del sujeto obligado en cuanto a la implementación y aplicación del sistema de manejo de datos personales, en posesión del sujeto obligado.

Las fechas exactas se les notificarán a los enlaces de Transparencia con al menos una semana de anticipación a las fechas estimadas con la intención de que éstos las difundan con los interesados en asistir a las capacitaciones.