

**DOCUMENTO DE SEGURIDAD
PARA LA PROTECCIÓN DE DATOS PERSONALES
DEL
SERVICIO ESTATAL DEL EMPLEO Y
CAPACITACIÓN PARA EL TRABAJO
(SEECAT) 2026**

Contenido

Introducción	3
Glosario de términos comunes.....	5
Objetivos del Documento de Seguridad del SEECAT.....	8
Responsabilidades dentro del Documento de Seguridad del SEECAT.....	8
I. El inventario de datos personales y de los sistemas de tratamiento.....	10
II. Las funciones y obligaciones de las personas que traten datos personales.....	11
III. Análisis de Riesgos.....	13
IV. Análisis de Brecha.....	17
V. Plan de Trabajo.....	19
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad.....	24
VII. Programa de capacitación.....	26
VIII. Actualización del Documento de Seguridad.....	27
Anexos.....	28

Introducción

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el estado de Quintana Roo (LPDPPSOQROO) en su última reforma publicada el 25 de noviembre de 2025 en el Periódico Oficial del estado, menciona que dicha ley tiene por objeto garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de los responsables (sujetos obligados).

En su artículo Tercero, fracción XXXI, la LPDPPSOQROO señala que son sujetos obligados por esta ley cualquier autoridad, entidad, órgano y organismo de los Poderes Legislativo, Ejecutivo y Judicial, Municipios, Órganos Constitucionales Autónomos, fideicomisos y fondos públicos en el ámbito estatal o municipal.

En ese sentido, como órgano desconcentrado de la Secretaría del Trabajo y Previsión Social del estado de Quintana Roo, el Servicio Estatal del Empleo y Capacitación para el Trabajo de Quintana Roo, en lo subsecuente SEECAT, es sujeto obligado de la LPDPPSOQROO y, por ello, debe observar lo dispuesto por dicho instrumento normativo en el tratamiento de datos personales que lleve a cabo.

De acuerdo con lo dispuesto por los artículos 11 y 30, de la LPDPPSOQROO, el SEECAT deberá implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en dicha Ley, la cual dispone que el tratamiento de datos personales que realicen los sujetos obligados estará regido por nueve principios y cuatro deberes. Los nueve principios son: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, transparencia y responsabilidad en el tratamiento de los datos personales; mientras que los deberes son el de seguridad, confidencialidad, integridad y disponibilidad. Estos principios, deberes y derechos imponen una serie de obligaciones para los sujetos regulados por la LPDPPSOQROO, cuya finalidad es que el tratamiento se realice garantizando la protección de los datos personales, con el objeto de respetar el derecho a la autodeterminación informativa de los titulares.

Asimismo, la LPDPPSOQROO detalla el alcance y los procedimientos para el ejercicio de los cuatro derechos que el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce a los titulares de los datos personales: acceso, rectificación, cancelación y oposición (derechos ARCO).

En específico, con relación al deber de seguridad, el artículo 30 de la LPDPPSOQROO señala que el responsable del tratamiento deberá **establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico** para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Al respecto, el artículo 32 de la LPDPPSOQROO señala lo siguiente:

Artículo 32. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

- I. *Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;*
- II. *Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;*
- III. *Elaborar un inventario de datos personales y de los sistemas de tratamiento de datos personales;*
- IV. *Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;*
- V. *Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;*
- VI. *Elaborar un plan de trabajo 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;*
- VII. *Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y*
- VIII. *Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.*

Por su parte, el artículo 35 de la LPDPPSOQROO establece como una obligación la elaboración de un documento de seguridad, que se define -según la fracción XV del artículo 4 de la misma ley - como el 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.

De conformidad con el artículo 35 de la LPDPPSOQROO, el documento deberá contener, al menos, la siguiente información:

- I. El inventario de datos personales y de los sistemas de tratamiento;
- II. Las funciones y obligaciones de las personas que traten datos personales;
- III. El análisis de riesgos;
- IV. El análisis de brecha;
- V. El plan de trabajo;
- VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
- VII. El programa general de capacitación.

En ese sentido, en cumplimiento de las obligaciones antes descritas, en el mes de marzo de 2024, el Comité de Transparencia del SEECAT, aprobó, el presente Documento de Seguridad, el cual deberá actualizarse cuando:

- Se produjeran modificaciones sustanciales en el nivel de riesgo.

- Como resultado de un proceso de mejora para mitigar la vulneración a la seguridad ocurrida.
- Como resultado de un proceso de mejora para el impacto de una vulneración a la seguridad ocurrida.
- Como resultado de un proceso de mejora, derivado del monitoreo y revisión del sistema de gestión para la seguridad de los datos personales que en su momento maneje el SEECAT.

A continuación, se presenta el Documento de Seguridad del Servicio Estatal del Empleo y Capacitación para el Trabajo (SEECAT) con los elementos informativos que establece el artículo 35 de la LPDPPSOQROO.

Glosario de términos comunes

Auditoría: Proceso sistemático, independiente 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 recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Bases de datos: Conjunto ordenado de datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Comité de Transparencia: Instancia a la que hace referencia el artículo 52 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el estado de Quintana Roo.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

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.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Documento de Seguridad: Instrumento que describe 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: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Evaluación de impacto en la protección de datos personales: Evaluación mediante la cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto 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.

Integridad: Garantizar la exactitud y la confiabilidad de la información de manera que no pueda ser modificada sin autorización, ya sea accidental o intencionadamente.

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

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.

Responsable: Sujeto obligado de la Ley General de Datos que decide el tratamiento de los datos personales.

Soporte: Medio de obtención o el formato de almacenamiento, ya sea físico o electrónico, en el que residen los datos personales tratados.

Plataforma Nacional: La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia.

Portabilidad de datos personales: Prerrogativa del titular de obtener una copia de los datos que ha proporcionado al responsable del tratamiento en un formato estructurado que le permita seguir utilizándolos.

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

Responsable: Sujeto obligado de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el estado de Quintana Roo, que decide sobre el tratamiento de los datos personales.

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.

SEECAT: Servicio Estatal del Empleo y Capacitación para el Trabajo de Quintana Roo.

Sujeto obligado: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal.

Titular: Persona física a quien corresponden los datos personales.

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

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

Unidad Administrativa: Área a la que se le confieren atribuciones específicas en el reglamento interno, estatuto orgánico o instrumento normativo equivalente que sea superior a un manual de organización.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 64 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el estado de Quintana Roo.

Objetivos del Documento de Seguridad del SEECAT

El presente Documento de Seguridad tiene como objetivos los siguientes:

1. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del SEECAT;
2. Cumplir con las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados para el estado de Quintana Roo, así como la normatividad que derive de los mismos;
3. Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, y
4. Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente una vez que el programa se haya implementado de manera integral en el SEECAT, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos.

Responsabilidades dentro del Documento de Seguridad del SEECAT

Con fundamento en lo dispuesto por los artículos 95 y 96, fracción II de la LPDPPSOQROO, que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano tendrá las siguientes funciones con relación a este Documento de Seguridad:

- I. Elaborar, aprobar, coordinar y supervisar el Documento de Seguridad, en conjunto con las áreas técnicas que estime necesario involucrar o consultar;
- II. Proponer cambios y mejoras al Documento de Seguridad, a partir de la experiencia de su implementación;
- III. Dar a conocer el Documento de Seguridad al interior del sujeto obligado;
- IV. Coordinar la implementación del Documento de Seguridad en las unidades administrativas del sujeto obligado;
- V. Asesorar a las unidades administrativas en la implementación de este Documento de Seguridad;
- VI. Presentar un informe anual al titular del SEECAT, en el que se describan las acciones realizadas para cumplir con lo dispuesto por este Documento de Seguridad;

- VII. Supervisar la correcta implementación del Documento de Seguridad;
- VIII. Elaborar, aprobar, coordinar y supervisar el programa anual de capacitación, en conjunto con las áreas técnicas que estime necesario involucrar o consultar, y
- IX. Las demás que de manera expresa señale el propio Documento de Seguridad.

El informe al que refiere la fracción VI anterior, deberá presentarse en las primeras dos semanas del mes de marzo de cada año y referirá al año inmediato anterior. Algunos de los elementos que pueden incluirse en el informe son:

- Estadística e información general sobre el cumplimiento de las obligaciones señaladas en el Documento de Seguridad para la Protección de Datos Personales por parte de las unidades administrativas;
- Acciones realizadas por el Comité de Transparencia y la Unidad de Transparencia para cumplir con las obligaciones específicas que establece el Documento de Seguridad para la Protección de Datos Personales, y
- Los resultados de las revisiones y auditorías.

Para que los objetivos planteados en la primera sección se logren con éxito, el Documento de Seguridad requiere del apoyo e impulso directo del más alto nivel de la institución. En ese sentido, se deberá hacer del conocimiento del Coordinador General, a fin de que tome las medidas necesarias para que el mismo se observe en SEECAT.

La intervención del Coordinador General tendrá la finalidad única de impulsar la debida implementación del Programa al interior del sujeto obligado, pero no podrá suplir ni afectar las funciones que otorgan los artículos 91 y 92 de la LPDPPSOQROO al Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la organización.

Asimismo, para que la implementación del Documento de Seguridad del SEECAT tenga como resultado el cumplimiento integral de las obligaciones que establece la LPDPPSOQROO, el Documento de Seguridad será de observancia obligatoria para todos los servidores públicos del sujeto obligado que en el ejercicio de sus funciones traten datos personales.

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

Para ello, resulta fundamental que el Documento de Seguridad se conozca al interior del SEECAT, por lo que el Comité de Transparencia se encargará de difundirlo entre los servidores públicos.

1. Alcance del Documento de Seguridad

El presente Documento de Seguridad aplicará a todas las unidades administrativas del SEECAT que realicen tratamiento de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que éstas efectúen en ejercicio de sus atribuciones.

Asimismo, en virtud de que uno de los objetivos del Documento de Seguridad es cumplir con las obligaciones establecidas en la LPDPPSOQROO, se cubrirán todos los principios, deberes y obligaciones que establece dicha norma para los responsables del tratamiento.

Las unidades administrativas que forman parte del SEECAT al 01 de enero de 2026, y que deberán observar el Documento de Seguridad, por tratar datos personales son las siguientes:

- I. Departamento de Desarrollo Humano y Administración de Recursos
- II. Departamento de Vinculación Laboral
- III. Departamento de Movilidad Laboral y Apoyos a Desempleados y Subempleados
- IV. Departamento de Atención y Servicios Chetumal
- V. Departamento de Atención y Servicios Cancún
- VI. Departamento de Atención y Servicios Playa del Carmen
- VII. Departamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

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

El artículo 32, fracción III de la LPDPPSOQROO establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la elaboración de un inventario de datos personales y de los sistemas de tratamiento y de acuerdo con la fracción I del artículo 35 de la Ley General de Datos Personales en Posesión de Sujetos Obligados, este inventario forma parte del documento de seguridad.

Para tal efecto el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:

- I. Finalidad del tratamiento
- II. Datos personales recabados
- III. Medios de obtención
- IV. Uso de los datos personales
- V. Forma de almacenamiento
- VI. Ubicación física o electrónica
- VII. Fundamento legal
- VIII. Cargo del servidor público responsable
- IX. Servidores públicos que tienen acceso a los sistemas de tratamiento
- X. Encargados en el tratamiento de datos personales (en su caso)
- XI. Transferencias de datos personales y su finalidad
- XII. Difusión de datos personales
- XIII. Plazo de conservación de los datos personales



A partir de lo anterior, el SEECAT con la finalidad de establecer y mantener las medidas de seguridad para la protección de los datos personales, elaboró un inventario de datos personales y de los sistemas de tratamiento, con la información básica del tratamiento de datos personales señalado por las Unidades Administrativas de esta dependencia.

El resultado del inventario fue que las ocho Unidades administrativas del SEECAT manejan en total 14 tratamientos de datos personales diferentes.

Los inventarios forman parte integral del presente documento de seguridad y se encuentran contenidos en el **Anexo 1**.

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

Es de precisar que el SEECAT, es el responsable sobre el tratamiento de los datos personales que se obtengan o utilicen con motivo de las facultades establecidas en su Ley Orgánica, y en ese sentido, todo el personal que por razón de sus funciones tenga acceso a los mismos debe atender al cumplimiento de los principios y deberes establecidos en los Artículos 11 y 30 de la LPDPPSOQROO, mismos que consisten en los siguientes:

PRINCIPIOS Y DEBERES.

Principios: Licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, transparencia y responsabilidad.

Deberes: Seguridad, confidencialidad, integridad y disponibilidad.

El artículo 32 fracción II y 35 fracción II de la LPDPPSOQROO establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la definición de las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

Con base a lo anterior se establecen de manera general las funciones y obligaciones que cualquier servidor público del SEECAT, observará al tratar datos personales:

Funciones:

- Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.
- Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos, a los que tienen acceso, se encuentren actualizados.
- Llevar un registro de los servidores públicos que accedan a los datos personales y llevar a cabo las acciones necesarias para que sea necesaria la autenticación de los usuarios.
- Mantener actualizada la relación de usuarios que traten datos personales.

- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, informar dicho incidente a la Unidad de Transparencia del SEECAT y llevar el registro de los hechos.

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad de carácter administrativo, físico y técnico necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como garantizando la confidencialidad, integridad y disponibilidad de los mismos.
- Atender los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.
- Dar aviso a su superior jerárquico, ante cualquier acción que pueda poner en riesgo los datos personales, y en general que pueda vulnerar la seguridad de los datos personales.
- Suscribir carta de confidencialidad para la protección de datos personales.
- Elaborar y actualizar el inventario de datos personales y de sistemas
- Elaborar y actualizar el aviso de privacidad
- Coadyuvar en el diseño e implementación del análisis de riesgo, análisis de brecha y en las Políticas Internas de Gestión y tratamiento de los datos personales del SEECAT.
- Participar en las acciones del Programa de Trabajo para establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso.
- Participar en las acciones de capacitación en materia de protección de datos personales.

De igual manera a continuación se determinan las obligaciones acordes a su nivel jerárquico:

Nivel jerárquico	Obligaciones para el tratamiento de datos personales
Jefes o encargados de Departamento (alto)	1) Supervisar el tratamiento realizado, así como acercarse a la Unidad de Transparencia del SEECAT, en caso de considerar que las medidas de seguridad sean las necesarias o requieran mejorarse para garantizar la integridad de los datos personales. 2) Llevar el control de altas y bajas de las servidoras y los servidores públicos que pueden tener acceso a los datos personales en tratamiento.
Jefes de oficina (medio)	Coadyuvar en la actualización de registros de las servidoras y los servidores públicos que realizan tratamientos; así como solicitar la cancelación de los permisos respectivos cuando una persona deje de laborar en el SEECAT.

Analistas (operativos)	Conocer las medidas de seguridad que debe implementar al tratar los datos personales y verificar qué medidas tomar en caso de que se vulnere los datos personales.
------------------------	--

Asimismo, el Comité de Transparencia es el área responsable de dar a conocer a las personas servidoras públicos del SEECAT el Documento de Seguridad para la Protección de Datos Personales, que se basa en un sistema de gestión, a fin de que el personal conozca sus funciones para el cumplimiento del sistema de gestión y las consecuencias de su incumplimiento.

Adicionalmente, conviene señalar que las funciones y obligaciones del personal que traten datos personales se encuentran definidas en la normatividad que rige el actuar del SEECAT.

III. Análisis de Riesgos

El artículo 32 fracción IV y 35 fracción III de la LPDPPSOQROO establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal responsable, entre otros.

Los datos personales a los que los servidores públicos del SEECAT tienen acceso en el ejercicio de sus atribuciones, se resguardan de manera física y electrónica, según las necesidades de la actividad para la cual se lleva a cabo su tratamiento.

Tanto para la protección de datos personales, como para los datos personales sensibles, determinados junto con su ciclo de vida por las Unidades Administrativas en el "Inventario de Datos Personales y de los Sistemas de Tratamiento" el SEECAT observa el máximo nivel de protección; es decir, sin discriminarlos por su valor o ciclo de vida, pues su vulneración podría tener como consecuencia negativa para los titulares de los datos personales la divulgación o incluso un daño en su esfera más íntima, daño moral o patrimonial, entre otros, siendo que el valor de los datos personales en la actualidad cobra cada día mayor relevancia por las implicaciones e información vinculados a ellos.

En este sentido, tanto los sistemas electrónicos como los medios a través de los cuales se resguardan de manera física los datos personales presentan diferentes particularidades en razón de las características de cada uno de ellos.

De forma general, el riesgo atiende a la combinación de la probabilidad de que por una vulneración ocurra una amenaza y de sus consecuencias desfavorables; de modo tal que, al determinar el riesgo en el escenario de la organización del SEECAT, se podrá realizar un estimado de las medidas de seguridad necesarias para preservar la información personal.

Durante el análisis de riesgos se realizó la revisión de todos los tratamientos de datos personales con la principal finalidad de asegurar el establecimiento de las medidas de seguridad adecuadas que garanticen el derecho a la protección de los datos personales.

Hay que destacar que para evaluar un riesgo fue necesario considerar todos los posibles escenarios en los que se haría efectivo, incluidos aquellos que implicaran un mal uso o abuso de los datos y las alteraciones técnicas o del entorno.

Es importante señalar que el Análisis de riesgos es el proceso para comprender la naturaleza del riesgo (peligro) y/o determinar su magnitud aceptable o tolerable. Consiste en averiguar el nivel de riesgo que el responsable o sujeto obligado está soportando. Para ello, tradicionalmente las metodologías proponen que se realice un inventario de activos, se determinen las amenazas, las probabilidades de que ocurran y los posibles impactos.

Los activos, las amenazas y las vulnerabilidades se combinan para generar riesgos.

El análisis de los riesgos busca calificar los riesgos identificados, a partir de la cuantificación de la probabilidad de ocurrencia y de sus consecuencias en términos de probabilidad y estadística (análisis cuantitativo), así como ordenando su importancia relativa (análisis cualitativo).

Metodología para el análisis de riesgos

Los elementos para analizar los riesgos de los recursos involucrados en el tratamiento de datos personales fueron:

1. Identificación de activos de apoyo.

Un activo es un recurso (ya sea material o físico, como documentos, servicios, prácticas, políticas, instalaciones; técnico como *software* o *hardware*, o humano como personas, etc.) que tiene valor para la organización del SEECAT y necesite, por tanto, ser protegido de potenciales riesgos. Los activos evaluados fueron aquéllos que se encontraban relacionados con el ciclo de vida de los datos personales previamente identificados y sus distintos tratamientos. Éstos se revisaron con el suficiente nivel de detalle para proveer la información que permitió hacer la valoración del riesgo.

2. Identificación de la amenaza

Para que algo pueda ser considerado amenaza, debe tener el potencial de dañar un activo y causar una vulneración a la seguridad. Las amenazas pueden ser de origen natural o humano, accidentales o deliberadas y provenir de adentro o de fuera del SEECAT.

AMENAZAS MÁS COMUNES A LOS ACTIVOS	
Fuego	Alteración de hardware
Agua	Alteración de software
Humedad	Fallas del equipo de cómputo
Fenómenos climáticos o meteorológicos	Saturación de los sistemas de información
Pérdida de suministro eléctrico	Uso no autorizado de equipo
Robo de equipo de cómputo	Uso de software copiado o falsificado
Robo de documentos físicos y electrónicos	Indisponibilidad del personal

3. Probabilidad de que ocurra una amenaza

No todas las amenazas tienen la misma posibilidad de que ocurran, debido a que habrá algunas que su presencia sea remota y otras que la probabilidad pueda ser alta. Por cada amenaza, la unidad administrativa, con base en su experiencia y conocimiento de los activos, debe dar aviso en aquellos casos que considere que hubo alguna variación en la probabilidad de que ocurra una amenaza para que el área especializada que corresponda determine si efectivamente el riesgo varió.

4. Conocimiento de vulnerabilidades por activo

La vulnerabilidad es la capacidad, las condiciones y características propias de los activos, que lo hacen susceptible a amenazas, con el resultado de sufrir un daño. Una vulnerabilidad es una debilidad en el funcionamiento o seguridad del activo y pueden ser identificadas en los siguientes ámbitos:

- Organizacionales.
- De procesos y procedimientos.
- De personal.
- Del ambiente físico.
- De la configuración de sistemas de información.
- Del *hardware*, *software* o equipo de comunicación.
- De la relación con prestadores de servicios.
- De la relación con terceros.

La presencia de vulnerabilidades por sí misma no causa daño, se requiere de una amenaza que la explote. Una vulnerabilidad que no se encuentre expuesta a una amenaza identificada posiblemente no requiera la implementación de un control, pero debe ser reconocida y monitoreada constantemente, o bien cuando surja algún cambio.

Por su parte, las medidas de seguridad usadas incorrectamente o con una mala implementación son una causa de vulnerabilidad. Una medida puede ser efectiva o no, dependiendo del contexto en el cual opera. Las vulnerabilidades pueden estar relacionadas a propiedades de los activos que a su vez pueden ser usadas para propósitos distintos a los que se habían destinado originalmente.

5 Estimado del impacto a los activos a través de la identificación del posible daño o consecuencia (evaluación del riesgo)

El riesgo se evaluó contemplando dos elementos básicos: el primero fue el estimado del impacto negativo, bajo, medio o alto, a los activos; y el segundo fue la identificación del

posible daño. Se determinó el daño que el riesgo pudiera causar a los activos, si era tolerable o debía mitigarse.

Algunos supuestos de vulneración son:

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

Riesgos detectados en el SEECAT

Debido a las circunstancias generales, tanto físicas como humanas, en las que las diversas unidades administrativas que integran el SEECAT tratan datos personales, se han identificado los siguientes posibles riesgos:

- Acceso de personas no autorizadas a los sistemas o plataformas oficiales.
- Falta de capacitación de los servidores públicos encargados del tratamiento de datos personales.
- Daño o fallas en las bases de datos físicas o almacenadas en medios electromagnéticos.
- Falta de contraseñas altamente efectivas o de mecanismos para identificar o autenticar a los usuarios.
- Mantenimiento insuficiente en los equipos de cómputo.
- Falla en equipos.
- Cambios de voltaje.
- Procesos carentes de formalidad para administración, acceso o cualquier tratamiento de datos personales.
- Carencia de un servidor o sistema que almacene los datos personales.
- La falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado, al área donde se almacenan o archivan los datos personales.

Ahora bien, es necesario hacer un análisis en el que se identifiquen las posibles consecuencias que pueden generarse por no dar cumplimiento a los principios y deberes establecidas en la LPDPPSOQROO.

RIESGO	POSIBLE CONSECUENCIA
Acceso de personas no autorizadas a los sistemas o plataformas oficiales.	Que personal no autorizado tenga acceso a la información y la divulgue, modifique o le dé un mal uso. Robo de información. Robo de identidad.
Falta de capacitación de los servidores públicos encargados del tratamiento de datos personales.	Pérdida de datos personales. Divulgación y transferencia indebida de los datos personales.

	Actualización de supuestos de infracción previstos en la normativa aplicable.
Daño o fallas en las bases de datos físicas o almacenadas en medios electromagnéticos.	Pérdida, destrucción y daño de los datos personales.
Falta de contraseñas altamente efectivas o de mecanismos para identificar o autenticar a los usuarios.	Pérdida, destrucción y daño de información. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Mantenimiento insuficiente. Falla en equipos. Cambios de voltaje.	Pérdida, destrucción y daño de información.
Procesos carentes de formalidad para administración, acceso o cualquier tratamiento de datos personales.	Pérdida, destrucción y daño de información. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Carencia de un servidor o sistema que almacene los datos personales. La falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado, al área donde se almacenan o archivan los datos personales.	Pérdida, destrucción y daño de información. Divulgación y transferencia de datos personales. Modificaciones no autorizadas

La metodología de la gestión de riesgos aplicada para el SEECAT, se puede apreciar en el **Anexo 2** de este documento.

IV. Análisis de Brecha

El artículo 32 fracción V y 35 fracción IV de la LPDPPSOQROO establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;

Una vez identificados los posibles riesgos a los que el SEECAT se encuentra susceptible de enfrentar, se deberán seleccionar e implementar las medidas de seguridad administrativas, técnicas o físicas orientadas a cumplir con el objetivo fijado para los riesgos.

El SEECAT ha considerado poner en marcha medidas de seguridad básicas para minimizar las vulneraciones a la seguridad de los datos personales y sistemas de tratamiento.

Las medidas de seguridad se abordarán bajo las siguientes categorías generales:

- A) Medidas de seguridad basadas en la cultura del personal.
- B) Medidas de seguridad en el entorno de trabajo físico.
- C) Medidas de seguridad en el entorno de trabajo digital.

Estas actividades relacionadas con el **análisis de brecha**, se detallan en el **Anexo 3**.

Medidas de seguridad existentes en el SEECAT

Podemos realizar el análisis de brecha, utilizando como base las medidas de seguridad existentes reportadas por las diversas unidades administrativas, las cuales consisten en lo siguiente:

- A) Medidas de seguridad existentes basadas en la cultura del personal.
 - Política de escritorio limpio
 - Hábitos de cierre y resguardo
 - Impresoras, escáneres, copiadoras y buzones limpios
 - Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico.
 - Fijar periodos de retención y destrucción de información
 - Personal informado sobre sus deberes mínimos de seguridad y protección de datos
 - Se fomenta la cultura de la seguridad de la información
 - Se difunden noticias en temas de seguridad
 - Se previene al personal sobre la Ingeniería Social
 - Se asegura la protección de datos personales en subcontrataciones
 - El personal realiza respaldos periódicos de los datos personales
- B) Medidas de seguridad existentes basadas en el entorno de trabajo físico.
 - Tener cerraduras y candados como medidas de seguridad para evitar el robo
 - Mantener en movimiento solo copias de la información, no el elemento original
 - Usar solo mensajería certificada
- C) Medidas de seguridad existentes basadas en el entorno de trabajo digital.
 - Actualizaciones al equipo de cómputo
 - medidas de seguridad para acceder al entorno de trabajo electrónico (uso de contraseñas y/o cifrado, administrar usuarios y accesos).
 - Uso de conexiones seguras

Medidas de seguridad faltantes y/o nuevas por implementar

A efecto de fijar la brecha entre las medidas de seguridad con las que cuenta el SEECAT y las faltantes y/o nuevas por implementar, se han identificado las siguientes:

- A) Medidas de seguridad por implementar basadas en la cultura del personal.
 - Gestión de bitácoras, usuarios y acceso
 - Mecanismos para eliminar de manera segura la información
 - Procedimientos para actuar ante vulneraciones a la seguridad de los datos personales
 - Tener un procedimiento de notificación de las vulneraciones a la seguridad de los datos personales.
 - Realizar revisiones y auditorías
- B) Medidas de seguridad faltantes basadas en el entorno de trabajo físico.
 - Medidas de seguridad para acceder al entorno de trabajo físico
 - Medidas de seguridad para evitar el robo (elementos disuasorios)
 - Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico.
- C) Medidas de seguridad por implementar basadas en el entorno de trabajo digital.
 - Revisar periódicamente el software instalado en el equipo de cómputo
 - Revisar la configuración de seguridad del equipo de cómputo
 - Reglas de navegación segura
 - Reglas para la divulgación de información

Es importante señalar que para este análisis se tiene claridad en cuales son los controles o medidas de seguridad que ya están funcionando de manera efectiva, así como las medidas identificadas como faltantes, lo cual permitirá elaborar un programa de trabajo que refleje las expectativas a lograr, las unidades administrativas involucradas y las fechas de compromiso para su implementación.

V. Plan de Trabajo

El artículo 32 fracción VI y 35 fracción V de la LPDPPSOQROO establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, elaborar un plan de trabajo 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;

Atendiendo a lo dispuesto en el análisis de riesgo y el análisis de brecha desarrollado en el presente documento y con la intención de definir las acciones a implementar para garantizar la protección de datos personales, se sugiere implementar las siguientes medidas de seguridad y plan de trabajo.

1) Medidas de seguridad por implementar

a) Basadas en la cultura del personal

Medida de seguridad	Descripción
Gestión de bitácoras para controlar el acceso a los sitios, medios de almacenamiento, formatos y equipo de cómputo.	Se deberá crear por cada Unidad Administrativa, un control o bitácora de los servidores públicos que tienen acceso a los archivos, equipo de cómputo y/o medios de almacenamiento electrónico; el control debe tener lo siguiente: • Registro para anotar el nombre y puesto del servidor público autorizado. • Fecha, hora de entrada y hora de salida del archivo o equipo de cómputo. • Registrar el expediente que se consultó. • Registrar el expediente o equipo de cómputo que se extrae, y fecha en la que se regresa. • Firma de conformidad del servidor público que accede al expediente o equipo de cómputo. • Firma de consentimiento del servidor público autorizado para llevar el control.
Mecanismos para eliminar de manera segura la información y evitar ser recuperado y visto por cualquier persona malintencionada.	Los documentos y otros medios físicos no deben simplemente desecharse una vez que ya no se utilizan, sino destruirse por ejemplo con triturado o incinerado. Tomar precauciones con los procedimientos de re-utilización, en ninguna circunstancia deberían utilizarse documentos con datos personales como "papel de reúso". Cuando el equipo de cómputo tenga que cambiar de dueño, por ejemplo, de un empleado a otro, es importante respaldar la información relevante para la organización y borrar completamente los datos que resguarda el equipo.
Procedimientos para actuar ante vulneraciones a la seguridad de los datos personales.	El tema de vulneraciones a la seguridad de los datos personales puede resultar particularmente complicado, la idea básica es disminuir la afectación a los titulares de los datos personales y a la institución. El Artículo 38 de la LPDPPSOQROO establece como vulnerables de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes: - La pérdida o destrucción no autorizada; - El robo, extravío o copia no autorizada; - El uso, acceso o tratamiento no autorizado, o - El daño, la alteración o modificación no autorizada.

	Por eso, se requiere tomar medidas como: • Tener un procedimiento de notificación: En caso de que ocurra una vulneración a la seguridad <i>el servidor público deberá avisar de manera inmediata al jefe de departamento al cual este adscrito</i>, el deberá evaluar qué información se afectó y los medios para notificar a los titulares de lo ocurrido, esto con el fin de alertarlos y que tomen precauciones. • Realizar revisiones: Se debe considerar la revisión periódica (semestral o anual) a la institución por un especialista en temas de seguridad para que éste realice evaluaciones y recomendaciones, o en su caso por el personal designado por el titular del SEECAT. Este tipo de revisiones podrían ayudar a revelar malas prácticas en el tratamiento de datos personales o la existencia de vulneraciones a la seguridad no detectadas. Los resultados de cualquier evaluación deben informarse a los empleados involucrados en el tratamiento de datos personales.
--	--

b) Basadas en el entorno del trabajo físico

Medida de seguridad	Descripción
Medidas de seguridad para acceder al entorno de trabajo físico	El acceso al entorno de trabajo físico debe ser sólo para personal autorizado, si no existen restricciones para el acceso, se corre el riesgo de que los datos personales sean robados o manipulados. De manera particular, ninguna persona sin autorización debería poder acercarse al equipo de cómputo, archiveros con datos personales, o a cualquier otro medio de almacenamiento. Para esto se deben considerar medidas como: • Mantener bitácoras de personas ajenas a la institución que accedan al entorno de trabajo: Es importante mantener un registro de todos los que ingresan y salen.
Medidas de seguridad para evitar el robo	Se deben establecer medidas con las cuales se minimice el riesgo de que alguien robe información fácilmente. Por ejemplo:

	Elementos disuasorios: Existen medidas de seguridad que reducen de manera significativa el interés de un atacante, por ejemplo, alarmas.
--	---

c) Basadas en el entorno de trabajo digital.

Medida de seguridad	Descripción
Revisar periódicamente el software instalado en el equipo de cómputo	Es importante revisar periódicamente qué tipos de programas se encuentran instalados en el equipo de cómputo, para verificar que se esté utilizando sólo software autorizado y evitar la instalación de software no deseado. Es de especial importancia evitar el uso de software para "bajar" o compartir archivos en equipos de cómputo de la organización, o con otros dispositivos personales, como tabletas o celulares, no sólo para evitar infringir la ley de derechos de autor, sino porque este software puede dar acceso a la información de un equipo a personas malintencionadas. También se debe vigilar que no se tenga instalado software sin licencia o "pirata", ya que éste podría estar infectado o simplemente no operar como el original y causar pérdida de información.
Revisar la configuración de seguridad del equipo de cómputo	El equipo de cómputo, el software y en algunas ocasiones los medios de almacenamiento electrónico tienen configuraciones que permiten incrementar su nivel de seguridad. El responsable de tecnologías de la información del SEECAT deberá habilitar las opciones de seguridad que permita a los equipos estar más seguros, por ejemplo, encender el firewall o habilitar las actualizaciones automáticas del antivirus. Es conveniente que todos los equipos del SEECAT, ya sean fijos o portátiles, mantengan un mismo nivel de configuración de seguridad.
Implementar medidas de seguridad para navegar en entornos digitales	El uso cotidiano de los equipos de cómputo y de los entornos digitales hace que se den por obvias algunas conductas que podrían representar riesgo a los datos personales, por ello se deben implementar medidas de seguridad como: ● Reglas de navegación segura: Sólo se deben revisar sitios web esenciales para la operatividad del SEECAT, evitando navegar en sitios no relacionados y mucho menos en sitios de riesgo como son los de descarga de contenido que violan los derechos de autor o pornográficos. Todos los empleados deben estar informados de

	los riesgos a los que se exponen por visitar sitios web que no son relevantes para sus funciones, también se les debe informar del peligro relacionado a la descarga de contenido, y la ventaja de verificar que el protocolo de conexión a los sitios web sea seguro, es decir, verificar que en la dirección web aparezca https y la imagen de un candado, en lugar de que sólo sea http. • Reglas para la divulgación de información: Antes de enviar información a un tercero, almacenarla en cuentas de cómputo en la nube, publicarla en un sitio web, o compartirla en redes sociales, se debe evaluar si esta acción no está poniendo en riesgo a titulares o a personal de la organización.
--	--

2) Plan de trabajo

Acciones	Responsable	Fecha de implementación
Implementar el uso de bitácoras para controlar el acceso de persona autorizado del SEECAT a los sitios, medios de almacenamiento, formatos y equipo de cómputo.	Jefes o encargados de Departamento del SEECAT.	Junio de 2026
Eliminar de manera segura la información que ya no se utiliza, mediante el triturado	Todas la Unidades Administrativas del SEECAT que manejen datos personales	Junio de 2026
Evitar la re-utilización de documentos con datos personales como "papel de reúso".	Todas la Unidades Administrativas del SEECAT que manejen datos personales	Junio de 2026
Respalidar la información relevante para la institución y borrar completamente los datos que resguarda el equipo de cómputo, cuando éste tenga que cambiar de dueño o usuario.	Todas la Unidades Administrativas del SEECAT que manejen datos personales	Junio de 2026
Elaborar un formato para reportar vulneraciones a la seguridad de los datos personales.	Unidad de Transparencia	Junio de 2026

Realizar revisiones periódicas a la seguridad de la protección de datos personales de la institución.	Jefes o encargados de Departamento del SEECAT.	Junio de 2026
Implementar bitácoras para controlar el acceso de personas ajenas a la institución.	Jefes o encargados de Departamento del SEECAT.	Junio de 2026
Presupuestar la contratación de la instalación de alarmas en las oficinas como medida de seguridad para evitar el robo de archivos y bienes de la institución.	Departamento de Desarrollo Humano y Administración de Recursos.	Abril de 2026
Revisar periódicamente el software instalado y la configuración de seguridad del equipo de cómputo	Responsable de Tecnologías de la Información del SEECAT.	Junio de 2026
Capacitar a los servidores públicos del SEECAT, sobre la importancia de implementar medidas de seguridad para navegar en entornos digitales	Responsable de Tecnologías de la Información del SEECAT.	Junio de 2026

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

El artículo 32 fracción VII y 35 fracción VI de la LPDPPSOQROO establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, implementar de manera periódica mecanismos de monitoreo y revisión de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales

En el presente documento de seguridad para la protección de datos personales, se detallan las acciones que establecen el mantenimiento de las medidas de seguridad en las cuales de manera general se destaca que el objeto de estas es la protección de los datos personales.

Para ello, con la finalidad de mantener un monitoreo y revisión de las medidas de seguridad, se llevarán a cabo de manera permanente las acciones siguientes:

1. La Unidad de Transparencia llevará un monitoreo del cumplimiento por parte de los servidores públicos que intervengan en las actividades detalladas en el Plan de Trabajo del presente documento.
2. Se mantendrá actualizado el inventario de datos personales y de los sistemas de tratamiento de estos.

3. El encargado de Tecnologías de la Información mantendrá monitoreados los esquemas de seguridad implementados para la infraestructura de tecnología de la información, comunicaciones y sistemas que permitan garantizar conexiones seguras, tanto al exterior como al interior del Instituto.

4. Para garantizar el cumplimiento de las políticas en materia de protección de datos personales establecidas en el presente documento de seguridad, el mismo se publicará en el microsítio del SEECAT y se enviará por medios electrónicos a los servidores públicos de la dependencia.

5. Se llevarán a cabo diversas medidas de seguridad físicas para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento mediante las siguientes actividades:

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

6. En relación con el monitoreo el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua. En este sentido, las acciones a monitorear son las siguientes:

- Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica entre otras;
- Las nuevas amenazas que podrían estar activadas dentro y fuera de la organización y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas pasadas que vuelvan a surgir;
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.

VII. Programa de capacitación

El artículo 32 fracción VIII y 35 fracción VII de la LPDPPSOQROO establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Con base a lo anterior se plantea generar un programa anual para desarrollar la cultura en seguridad de la información, conforme a los siguientes ejes:

- a) **Programas a corto plazo** para la difusión en general de la protección de datos personales en la institución y su importancia en el entorno laboral; se prevé proporcionar una introducción al marco teórico y legal en el tema y proporcionar ejemplos e insumos que le permitan a la servidora pública y al servidor público comprender la importancia de la protección de datos personales, tanto en el rol de servidora pública o servidor público como el de titular de la Unidad Administrativa; así como identificar hábitos que ponen en riesgo la protección de datos personales.
- b) **Programas a mediano plazo** que tienen por objetivo capacitar al personal de manera específica respecto a sus funciones y responsabilidad en el tratamiento y seguridad de los datos personales; se impartirán cursos o talleres que permitan a las servidoras públicas y a los servidores públicos identificar los procedimientos a seguir en la atención de solicitudes de derechos ARCO, la actualización de avisos de privacidad e inventarios de tratamiento y para la revisión y actualización de medidas de seguridad para reducir los riesgos de vulneración de datos personales.
- c) **Programa general a largo plazo** que tiene por objetivo incluir la seguridad en el tratamiento de los datos personales dentro de la cultura de organización de la Institución.
- d) Asimismo, el personal de enlace de cada Unidad Administrativa del SEECAT estará en capacitación constante por medio de cursos y/o talleres presenciales o en línea por parte del Instituto de Acceso a la Información y Protección de Datos Personales, tanto estatal como federal.

El Programa Anual de Capacitación en materia de Datos Personales deberá ser presentado a más tardar en la última sesión ordinaria de cada año del Comité de Transparencia, y deberá diseñarse de tal forma que permita el cumplimiento de las metas señaladas, así como de las necesidades específicas que se detecten durante su implementación.

El Programa Anual de Capacitación del SEECAT, se detalla en el **Anexo 4**.

El Programa Anual de Capacitación del SEECAT, se detalla en el **Anexo 4**.

VIII. Actualización del Documento de Seguridad

El artículo 36 de la LPDPPSOQROO establece que el responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:

- I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
- II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, e
- IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En ese sentido, cuando se actualice alguno de los supuestos antes citados, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia con el objeto de que éste determine si considera procedente la actualización del presente documento de seguridad.

Todos los sistemas de tratamiento que integran el documento de seguridad del SEECAT deben mantenerse actualizados; sin embargo, se entenderá que las modificaciones implican la necesidad de actualizar el documento de seguridad cuando al adecuarse el nivel de riesgo reportado las medidas de seguridad resulten insuficientes.

El presente documento de seguridad fue elaborado y autorizado por:

ELABORÓ	AUTORIZÓ
	
ING. MARCO ANTONIO MARTÍNEZ AGUILAR Titular de la Unidad de Transparencia	LIC. TAYDE GUADALUPE ROJAS CAMPOS Encargada de la Coordinación General del SEECAT

Aprobación del Documento de Seguridad: 26 de junio de 2024, en la segunda sesión ordinaria del Comité de Transparencia del SEECAT.

Primera actualización: 30 de abril de 2025, en la segunda sesión ordinaria del Comité de Transparencia del SEECAT.

Segunda actualización: 25 junio 2026 en la segunda sesión ordinaria del Comité de Transparencia del SEECAT.

ANEXOS

ANEXO 1: Inventario de datos personales y de los sistemas de tratamiento.

Inventario de datos personales

No.	Denominación del tratamiento de Datos Personales	Unidad Administrativa
1	Expediente único del personal	Desarrollo Humano y Administración de Recursos
2	Reloj checador	
3	Administrar el presupuesto de subsidios del Programa de Apoyo al Empleo (PAE)	
4	Buscadores de empleo atendidos por Vinculación Laboral.	Departamento de Vinculación Laboral, Departamento de Atención y Servicios Chetumal, Departamento de Atención y Servicios Cancún, Departamento de Atención y Servicios Playa del Carmen.
5	Empleadores usuarios de Vinculación Laboral	Departamento de Vinculación Laboral, Departamento de Atención y Servicios Chetumal, Departamento de Atención y Servicios Cancún, Departamento de Atención y Servicios Playa del Carmen.
6	Buscadores de trabajo participantes en el Programa Capacítate y Empléate	Departamento de Atención y Servicios Chetumal, Departamento de Atención y Servicios Cancún, Departamento de Atención y Servicios Playa del Carmen. Departamento de Apoyos a Desempleados y Subempleados.
7	Representantes de centros Capacitadores participantes en el Programa Capacítate y Empléate	Departamento de Atención y Servicios Chetumal, Departamento de Atención y Servicios Cancún, Departamento de Atención y Servicios Playa del Carmen. Departamento de Movilidad Laboral y Apoyos a Desempleados y Subempleados.
8	Buscadores de empleo aspirantes al Subprograma Movilidad laboral	Departamento de Movilidad Laboral y Apoyos a Desempleados y Subempleados.

13	Supervisiones a participantes del Programa de Apoyo al Empleo	Departamento de Vinculación
14	Lista de atendidos del Programa de Apoyo al Empleo	
15	Eventos Públicos	

Sistemas de Tratamiento de los datos personales

1 Expediente único del personal	
Finalidad del tratamiento	Integrar el expediente único de personal del SEECAT, a fin de realizar los trámites administrativos y fiscales.
Datos personales recabados	Nombre completo, RFC, domicilio, escolaridad, CURP y experiencia laboral. En ningún caso se tiene acceso a Datos Personales Sensibles.
¿Cómo se obtienen los datos personales?	Directamente del titular, con la presencia física.
Uso de los datos	Mantener actualizado el expediente único del personal.
Formato de almacenamiento	Físico
Descripción general de la ubicación física y/o electrónica de los datos personales	Archivero ubicado dentro de la oficina del Departamento de Desarrollo Humano y Administración de Recursos, únicamente el Coordinador General del SEECAT, jefa de Departamento de Desarrollo Humano y Administración de Recursos, jefa de Oficina de Recursos Humanos cuenta con acceso.
Fundamento legal	Artículo 3, fracciones X, XI y XXXIV, 11 de la LPDPPSOEQROO.
Cargo del servidor público responsable	Jefa de Departamento de Desarrollo Humano y Administración de Recursos.
Servidores públicos que tienen acceso a los sistemas de tratamiento	Coordinador General del SEECAT, jefa de Departamento de Desarrollo Humano y Administración de Recursos, jefa de Oficina de Recursos Humanos.
¿Intervienen encargados en el tratamiento de datos personales?	Si, la Dirección Administrativa de la Secretaría del Trabajo y Previsión Social del estado de Quintana Roo.
¿Se realizan transferencias de datos personales y con qué finalidad?	Sí se realizan transferencias de Datos Personales a la Secretaría del Trabajo y Previsión Social del estado de Quintana Roo, y cuando sea necesario para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
¿Se difunden los datos personales?	No
¿Cuál es el plazo de conservación de los datos personales?	8 años

2 Reloj checador	
Finalidad del tratamiento	Llevar un control de asistencia de los servidores públicos que ocupen plazas con nivel de Intendente, Oficial de Partes, Analista, Auxiliar de Correspondencia, Auxiliar de Mantenimiento, consejera de Empleo, jefe de Oficina, Analista Técnico, secretaria, Promotor Laboral, Operador Auxiliar en Recursos Materiales, secretaria ejecutiva y Asistente Ejecutivo B.
Datos personales recabados	Nombre completo, fotografía, turno/horario, departamento y huella dactilar. Se recaba el Dato Personal Sensible de la huella dactilar.
¿Cómo se obtienen los datos personales?	Directamente del titular, con la presencia física.
Uso de los datos	Llevar un control de entradas y salidas del personal para reportar a la Dirección Administrativa de la STyPS, para los estímulos y recompensas correspondientes.
Formato de almacenamiento	Electrónico y físico (Base de datos en formatos Excel y PDF).
Descripción general de la ubicación física y/o electrónica de los datos personales	En el Departamento de Desarrollo Humano y Administración de Recurso y en la computadora asignada a la Oficina de Recursos Humanos.
Fundamento legal	Artículo 3, fracciones X, XI y XXXIV, 11 de la LPDPPSOEQROO. Artículos 35, 36 y 37 del Reglamento de Condiciones Generales de Trabajo de Los Trabajadores al Servicio del Poder Ejecutivo del Estado de Quintana Roo.
Cargo del servidor público responsable	Jefa de Departamento de Desarrollo Humano y Administración de Recursos.
Servidores públicos que tienen acceso a los sistemas de tratamiento	Coordinador General del SEECAT, jefa de Departamento de Desarrollo Humano y Administración de Recursos, jefa de Oficina de Recursos Humanos.
¿Intervienen encargados en el tratamiento de datos personales?	Si, la Dirección Administrativa de la Secretaría del Trabajo y Previsión Social del estado de Quintana Roo.
¿Se realizan transferencias de datos personales y con qué finalidad?	Sí se realizan transferencias de Datos Personales a la Secretaría del Trabajo y Previsión Social del estado de Quintana Roo, y cuando sea necesario para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
¿Se difunden los datos personales?	No
¿Cuál es el plazo de conservación de los datos personales?	7 años

3 Administrar el presupuesto de subsidios del Programa de Apoyo al Empleo (PAE)	
Finalidad del tratamiento	Cotejar el nombre completo, cargo y firma de la autoridad estatal y de los responsables de Administrar Subsidios designados en el formato PAE-RF1 para administrar los recursos de subsidios en el marco de los servicios, programas y estrategias del Servicio Nacional de Empleo.

	Transferir a la Institución Financiera para el trámite de microfilmación de firmas para la operación de la subcuenta pagadora contratada en el marco de la operación del PAE.
Datos personales recabados	Nombre, domicilio, CURP, fotografía y firma. No se recaban Datos Personales Sensibles.
¿Cómo se obtienen los datos personales?	Directamente del titular, con la presencia física.
Uso de los datos	Para gestionar la liberación de recursos de operación del PAE.
Formato de almacenamiento	Físico y Electrónico (Base de datos en formatos Excel, Adobe Acrobat, entre otros).
Descripción general de la ubicación física y/o electrónica de los datos personales	Carpeta compartida del Departamento de Desarrollo humano y Administración de Recursos, en los servidores del SEECAT, únicamente personal facultado por la Coordinación General cuenta con acceso a dicha carpeta.
Fundamento legal	Artículo 3, fracciones X, XI y XXXIV, 11 de la LPDPPSOEQROO. El artículo 38 del Reglamento Interior de la Secretaría del Trabajo y Previsión Social del Gobierno del Estado de Quintana Roo.
Cargo del servidor público responsable	Jefa de Departamento de Desarrollo Humano y Administración de Recursos.
Servidores públicos que tienen acceso a los sistemas de tratamiento	Coordinador General del SEECAT, jefa de Departamento de Desarrollo Humano y Administración de Recursos, jefe de Oficina Financiera. (federales)
¿Intervienen encargados en el tratamiento de datos personales?	No
¿Se realizan transferencias de datos personales y con qué finalidad?	Sí, podrán ser transferidos a la Institución Financiera para el trámite de microfilmación de firmas para la operación de la subcuenta pagadora contratada en el marco de la operación del PAE. Se informa que no se realizarán transferencias adicionales de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
¿Cuál es el plazo de conservación de los datos personales?	9 años

4 Buscadores de empleo atendidos por Vinculación Laboral.

Finalidad del tratamiento	Los datos personales que proporcionen de manera presencial en las oficinas del SEECAT o vía telefónica, serán tratados para que sea considerado como candidato en un proceso de reclutamiento, evaluación y/o selección de personal por lo que serán utilizados con fines de registro, seguimiento y control e informes sobre la población atendida mediante Vinculación Laboral.
Datos personales recabados	Nombre completo, CURP, edad, teléfono particular y/o de referencia, correo electrónico, domicilio, escolaridad, firma autógrafa, otros estudios, idiomas adicionales, conocimientos con los que cuenta, experiencia, expectativa laboral, fecha de ingreso y fecha de término, lengua indígena que habla, ingreso mensual neto, sexo, fecha de nacimiento, lugar de nacimiento, nacionalidad, escuela o instituto, año de egreso, entidad federativa, disponibilidad para viajar, competencias y redes sociales.

	Se recaban Datos Personales Sensibles de discapacidad con el fin de proporcionar un mejor servicio mediante una canalización eficaz.
¿Cómo se obtienen los datos personales?	Directamente del titular, con la presencia física, vía telefónica y por sistemas informáticos.
Uso de los datos	Para fines de registro, seguimiento y control e informes sobre la población atendida mediante Vinculación Laboral.
Formato de almacenamiento	Electrónico (Hoja de Cálculo Google Drive, Sistema de Intermediación Laboral Para Atención Personalizada -SILAP-).
Descripción general de la ubicación física y/o electrónica de los datos personales	Sistema de Intermediación Laboral Para Atención Personalizada (SILAP) https://silap.empleo.gob.mx/PortalDigital Carpeta compartida del Departamento de Vinculación Laboral, en los servidores del SEECAT, únicamente personal facultado por la Coordinación General cuenta con acceso a dicha carpeta.
Fundamento legal	Artículo 3, fracciones X, XI y XXXIV, 11 de la LPDPPSOEQROO.
Cargo del servidor público responsable	Jefe de Departamento de Vinculación Laboral
Servidores públicos que tienen acceso a los sistemas de tratamiento	<i>Coordinador General del SEECAT, jefe de Departamento de Vinculación Laboral, jefe de Departamento de Atención y Servicios Chetumal, jefe de Departamento de Atención y Servicios Cancún, jefe de Departamento de Atención y Servicios Playa del Carmen, jefe de Oficina de Vinculación Laboral, jefe de Oficina Community Manager, jefe de Oficina de Sistemas, Auxiliar Administrativo, Analista Técnico, Concertadores y Concertadoras de Empresas, consejeros y consejeras Laborales.</i>
¿Intervienen encargados en el tratamiento de datos personales?	No.
¿Se realizan transferencias de datos personales y con qué finalidad?	Sí, los Datos Personales podrán ser transferidos a los empleadores con el fin de apoyar su colocación en algún puesto vacante afín a su perfil laboral. Se informa que no se realizarán transferencias adicionales de datos personales, salvo aquellas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
¿Cuál es el plazo de conservación de los datos personales?	7 años

5 Empleadores usuarios de Vinculación Laboral	
Finalidad del tratamiento	Los datos personales que proporcionen de manera presencial en las oficinas del SEECAT o vía telefónica, serán con fines de registro en el Sistema de Intermediación Laboral Para Atención Personalizada (SILAP), Portal del Empleo, seguimiento, vinculación laboral y control e informes sobre los empleadores atendidos.
Datos personales recabados	Nombre completo, RFC, CURP, domicilio, teléfono particular y celular, correo electrónico y firma autógrafa. No se recaban Datos Personales Sensibles.
¿Cómo se obtienen los datos personales?	Directamente del titular, con la presencia física, vía telefónica, por sistemas informáticos o correo electrónico.
Uso de los datos	Para enviar a las empresas candidatos a cubrir vacantes, registro en el Sistema de Intermediación Laboral Para Atención

	Personalizada (SILAP), Portal del Empleo, seguimiento, vinculación laboral y control e informes sobre los empleadores atendidos.
Formato de almacenamiento	Electrónico (formatos Excel, Anexo IV Términos y condiciones, Sistema de Intermediación Laboral Para Atención Personalizada - SILAP-).
Descripción general de la ubicación física y/o electrónica de los datos personales	Sistema de Intermediación Laboral Para Atención Personalizada (SILAP) https://silap.empleo.gob.mx/PortalDigital Carpeta compartida del Departamento de Vinculación, en los servidores del SEECAT, únicamente personal facultado por la Coordinación General cuenta con acceso a dicha carpeta.
Fundamento legal	Artículo 3, fracciones X, XI y XXXIV, 11 de la LPDPPSOEQROO.
Cargo del servidor público responsable	Jefe de Departamento de Vinculación Laboral
Servidores públicos que tienen acceso a los sistemas de tratamiento	Coordinador General del SEECAT, jefe de Departamento de Vinculación Laboral, jefe de Departamento de Atención y Servicios Chetumal, jefe de Departamento de Atención y Servicios Cancún, jefe de Departamento de Atención y Servicios Playa del Carmen, jefa de Oficina de Vinculación Laboral, jefe de Oficina Community Manager, jefe de Oficina de Sistemas, Auxiliar Administrativo, Analista Técnico, Concertadores y Concertadoras de Empresas, consejeros y consejeras Laborales.
¿Intervienen encargados en el tratamiento de datos personales?	No.
¿Se realizan transferencias de datos personales y con qué finalidad?	No se realizarán transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
¿Cuál es el plazo de conservación de los datos personales?	7 años.

6 Buscadores de trabajo participantes en el Programa Capacítate y Empléate

Finalidad del tratamiento	Los datos personales que proporcione mediante los formatos inherentes al Programa <i>Capacítate y Empléate</i> , serán tratados para su participación en algún curso de capacitación del Programa <i>Capacítate y Empléate</i> , por lo que serán utilizados con fines de registro, seguimiento, control de asistencia, trámite y entrega de apoyos, emisión de constancias de capacitación y control e informes sobre la población atendida y beneficiada.
Datos personales recabados	Nombre completo, CURP, edad, estado civil, teléfono particular y/o de referencia, correo electrónico, domicilio, escolaridad, firma autógrafa, otros estudios, idiomas adicionales, conocimientos con los que cuenta, experiencia, expectativa laboral, lengua indígena que habla, Clave Bancaria Estandarizada. Se recaban Datos Personales Sensibles de discapacidad con el fin de proporcionarle un mejor servicio mediante una canalización eficaz hacia un curso de capacitación.
¿Cómo se obtienen los datos personales?	Directamente del titular, con la presencia física
Uso de los datos	Con fines de registro, seguimiento, control de asistencia, trámite y entrega de apoyos, emisión de constancias de capacitación y

	control e informes sobre la población atendida y beneficiada en el <i>Programa Capacítate y Empléate</i> .
<i>Formato de almacenamiento</i>	Físico y Electrónico (Base de datos en formatos Excel).
<i>Descripción general de la ubicación física y/o electrónica de los datos personales</i>	Carpeta compartida en el Departamento de Apoyos a Desempleados y Subempleados, en los servidores del SEECAT, únicamente personal facultado por la Coordinación General cuenta con acceso a dicha carpeta.
<i>Fundamento legal</i>	Artículo 3, fracciones X, XI y XXXIV, 11 de la LPDPPSOEQROO.
<i>Cargo del servidor público responsable</i>	Jefe de Departamento Apoyos a Desempleados y Subempleados.
<i>Servidores públicos que tienen acceso a los sistemas de tratamiento</i>	Coordinador General del SEECAT, jefe de Departamento de Atención y Servicios Chetumal, jefe de Departamento de Atención y Servicios Cancún, jefe de Departamento de Atención y Servicios Playa del Carmen, jefa de Oficina de Apoyos Financieros y Capacitación, Concertadores de Empresas y consejeros Laborales.
¿Intervienen encargados en el tratamiento de datos personales?	No.
¿Se realizan transferencias de datos personales y con qué finalidad?	Los Datos Personales podrán ser transferidos entre Sujetos Obligados, específicamente con la Secretaría de Bienestar (SEBIEN), para fines de informar sobre la población atendida con recursos estatales. Se informa que no se realizarán transferencias adicionales de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
¿Cuál es el plazo de conservación de los datos personales?	9 años.

7 Representantes de centros Capacitadores participantes en el Programa Capacítate y Empléate

<i>Finalidad del tratamiento</i>	Los datos personales que proporcionen mediante los formatos inherentes al Programa Capacítate y Empléate, serán tratados para que sea considerada la Institución que representa como Centro de Capacitación en el Programa mencionado, con fines de registro, seguimiento y control e informes.
<i>Datos personales recabados</i>	Nombre completo, RFC, CURP, domicilio, teléfono, correo electrónico, puesto que ocupa y firma autógrafa. No se recaban Datos Personales Sensibles.
¿Cómo se obtienen los datos personales?	Directamente del titular, con la presencia física o por correo electrónico.
<i>Uso de los datos</i>	Para el registro, seguimiento y control e informes, de los Centros Capacitadores participantes en el Programa capacítate y Empléate.
<i>Formato de almacenamiento</i>	Físico y Electrónico (Base de datos en formatos Excel).
<i>Descripción general de la ubicación física y/o electrónica de los datos personales</i>	Carpeta compartida en el Departamento de Apoyos a Desempleados y Subempleados, en los servidores del SEECAT, únicamente personal facultado por la Coordinación General cuenta con acceso a dicha carpeta.

<i>Fundamento legal</i>	Artículo 3, fracciones X, XI y XXXIV, 11 de la LPDPPSOEQROO.
<i>Cargo del servidor público responsable</i>	Jefe de Departamento de Movilidad Laboral y Apoyos a Desempleados y Subempleados.
<i>Servidores públicos que tienen acceso a los sistemas de tratamiento</i>	Coordinador General del SEECAT, jefe de Departamento de Atención y Servicios Chetumal, jefe de Departamento de Atención y Servicios Cancún, jefe de Departamento de Atención y Servicios Playa del Carmen, jefa de Oficina de Apoyos Financieros y Capacitación, Concertadores de Empresas y consejeros Laborales.
¿Intervienen encargados en el tratamiento de datos personales?	No.
¿Se realizan transferencias de datos personales y con qué finalidad?	Atendiendo a los principios de licitud y proporcionalidad, se realizarán transferencias a los buscadores de trabajo participantes en el Programa de Apoyo al Empleo Estatal (PAEE), para fines de canalización. Se informa que no se realizarán transferencias adicionales de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
¿Cuál es el plazo de conservación de los datos personales?	9 años.

8 Buscadores de empleo aspirantes al Subprograma Movilidad laboral	
<i>Finalidad del tratamiento</i>	Los datos personales que nos proporcione a través del formato SNE-01 (Registro del Solicitante), serán tratados para que sea considerado como aspirante en el Subprograma Movilidad Laboral, por lo que serán utilizados con fines de registro, seguimiento, trámite y entrega de apoyos y control e informes sobre la población atendida y beneficiada.
<i>Datos personales recabados</i>	Nombre completo, CURP, edad, teléfono particular y/o de referencia, correo electrónico, domicilio, escolaridad, firma autógrafa, otros estudios, idiomas adicionales, conocimientos con los que cuenta, experiencia, expectativa laboral, lengua indígena que habla e ingreso mensual neto. Se recaban Datos Personales Sensibles de discapacidad con el fin de proporcionarle un mejor servicio mediante una canalización eficaz.
¿Cómo se obtienen los datos personales?	Directamente del titular, con la presencia física.
<i>Uso de los datos</i>	Con fines de registro, seguimiento, trámite y entrega de apoyos y control e informes sobre la población atendida y beneficiada en el Subprograma de Movilidad Laboral.
<i>Formato de almacenamiento</i>	Sistema de Intermediación Laboral para Atención Personalizada (SILAP). Módulo de Mecanismo de Movilidad Laboral (MMML). Físico y Electrónico (Base de datos en formatos Excel).
<i>Descripción general de la ubicación física y/o electrónica de los datos personales</i>	Carpeta compartida en el Departamento de Movilidad Laboral en los servidores del SEECAT, únicamente personal facultado por la Coordinación General cuenta con acceso a dicha carpeta.

<i>Fundamento legal</i>	Artículo 3, fracciones X, XI y XXXIV, 11 de la LPDPPSOEQROO.
<i>Cargo del servidor público responsable</i>	Jefe de Departamento de Movilidad Laboral.
<i>Servidores públicos que tienen acceso a los sistemas de tratamiento</i>	Coordinador General del SEECAT, jefa de Oficina de Formación Laboral y consejeros Laborales.
¿Intervienen encargados en el tratamiento de datos personales?	No.
¿Se realizan transferencias de datos personales y con qué finalidad?	Se informa que no se realizarán transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
<i>Ciclo de vida y riesgo inherente de los datos personales</i>	Permanente Al tratarse de datos personales contenidos en un sistema electrónico, los riesgos que por la propia naturaleza tendría dicho sistema son: el uso indebido de la información, la falla en los equipos electrónicos o en los sistemas; por ello, el SEECAT cuenta con un área soporte encargada de ejecutar acciones para garantizar la seguridad de la información. Al tratarse de datos personales resguardados físicamente, los riesgos existentes son la pérdida o uso indebido de la información, deterioro negligente, así como su destrucción; por ello, el SEECAT cuenta con un área soporte encargada de ejecutar acciones para garantizar la Seguridad de la información.
¿Cuál es el plazo de conservación de los datos personales?	7 años.

9 Buscadores de empleo aspirantes al Programa de Trabajadores Agrícolas Temporales México-Canadá.

<i>Finalidad del tratamiento</i>	Los datos personales que nos proporcione a través de entrevista y copia de documentos solicitados serán tratados para que sea considerado como aspirante en el Programa de Trabajadores Agrícolas Temporales México Canadá, por lo que serán utilizados con fines de registro, seguimiento, trámite y control e informes sobre la población atendida y beneficiada.
<i>Datos personales recabados</i>	Nombre completo, CURP, edad, estado civil, teléfono, domicilio, escolaridad, firma autógrafa, experiencia laboral, estado de salud, nombre de hijos y esposa.
	No se recaban Datos Personales Sensibles.
¿Cómo se obtienen los datos personales?	Directamente del titular, con la presencia física.
<i>Uso de los datos</i>	Serán utilizados con fines de registro, seguimiento, trámite y control e informes sobre la población atendida y beneficiada en el Programa de Trabajadores Agrícolas Temporales México Canadá.
<i>Formato de almacenamiento</i>	Sistema Informático de Movilidad Laboral (SIMOL) Físico y Electrónico (Base de datos en formatos Excel).

<i>Descripción general de la ubicación física y/o electrónica de los datos personales</i>	Carpeta compartida en el Departamento de Movilidad Laboral en los servidores del SEECAT, únicamente personal facultado por la Coordinación General cuenta con acceso a dicha carpeta.
<i>Fundamento legal</i>	Artículo 3, fracciones X, XI y XXXIV, 11 de la LPDPPSOEQROO.
<i>Cargo del servidor público responsable</i>	Jefe de Departamento de Movilidad Laboral y Apoyos a Desempleados y Subempleados.
<i>Servidores públicos que tienen acceso a los sistemas de tratamiento</i>	Coordinador General del SEECAT, Analista Técnico.
<i>¿Intervienen encargados en el tratamiento de datos personales?</i>	No.
<i>¿Se realizan transferencias de datos personales y con qué finalidad?</i>	Se informa que no se realizarán transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
<i>¿Cuál es el plazo de conservación de los datos personales?</i>	7 años.

10 Solicitudes de información	
<i>Finalidad del tratamiento</i>	Los datos personales recabados de manera presencial, por escrito, vía correo electrónico, telefónicamente o a través de la Plataforma Nacional de Transparencia, serán utilizados con fines de registro, seguimiento, respuesta a las Solicitudes de Información y control e informes sobre las solicitudes atendidas.
<i>Datos personales recabados</i>	Nombre completo, domicilio, número telefónico y correo electrónico. No se recaban Datos Personales Sensibles.
<i>¿Cómo se obtienen los datos personales?</i>	Directamente del titular, con la presencia física, vía telefónica, correo electrónico y sistemas informáticos.
<i>Uso de los datos</i>	Con fines de registro, seguimiento, respuesta a las Solicitudes de Información y control e informes sobre las solicitudes atendidas.
<i>Formato de almacenamiento</i>	Plataforma Nacional de Transparencia (PNT). Físico y Electrónico (Base de datos en formatos Excel).
<i>Descripción general de la ubicación física y/o electrónica de los datos personales</i>	La PNT resguarda a nivel nacional los datos de los usuarios que deseen solicitar información. Carpeta compartida en el Departamento de Departamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales en los servidores del SEECAT, únicamente personal facultado por la Coordinación General cuenta con acceso a dicha carpeta.
<i>Fundamento legal</i>	Artículo 3, fracciones X, XI y XXXIV, 11 y 135 de la LPDPPSOEQROO.
<i>Cargo del servidor público responsable</i>	Jefe de Departamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

<i>Servidores públicos que tienen acceso a los sistemas de tratamiento</i>	<i>Coordinador General del SEECAT, jefes de departamento de todas las áreas del SEECAT.</i>
¿Intervienen encargados en el tratamiento de datos personales?	No.
¿Se realizan transferencias de datos personales y con qué finalidad?	Se informa que no se realizarán transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
¿Cuál es el plazo de conservación de los datos personales?	7 años.

11 Solicitud para el ejercicio de los derechos ARCO

<i>Finalidad del tratamiento</i>	Los datos personales que nos proporcione a través del formato de Solicitud para el Ejercicio de los Derechos ARCO, serán utilizados con fines de registro, seguimiento, respuesta a las Solicitudes para el Ejercicio de los Derechos ARCO y control e informes sobre las solicitudes atendidas.
<i>Datos personales recabados</i>	Nombre completo, domicilio, número telefónico y correo electrónico, e identificación oficial. No se recaban Datos Personales Sensibles.
¿Cómo se obtienen los datos personales?	Directamente del titular, con la presencia física.
<i>Uso de los datos</i>	Con fines de registro, seguimiento, respuesta a las Solicitudes para el Ejercicio de los Derechos ARCO y control e informes sobre las solicitudes atendidas.
<i>Formato de almacenamiento</i>	Físico y Electrónico (Base de datos en formatos Excel).
<i>Descripción general de la ubicación física y/o electrónica de los datos personales</i>	Carpeta compartida en el Departamento de Departamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales en los servidores del SEECAT, únicamente personal facultado por la Coordinación General cuenta con acceso a dicha carpeta.
<i>Fundamento legal</i>	Artículo 3, fracciones X, XI y XXXIV, 11, 43, 44, 45, 46, 47; 52, 53, 54 Y 59 de la LPDPPSOEQROO.
<i>Cargo del servidor público responsable</i>	Jefe de Departamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.
<i>Servidores públicos que tienen acceso a los sistemas de tratamiento</i>	<i>Coordinador General del SEECAT, jefes de departamento de todas las áreas del SEECAT.</i>
¿Intervienen encargados en el tratamiento de datos personales?	No.
¿Se realizan transferencias de datos personales y con qué finalidad?	Se informa que no se realizarán transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.

¿Cuál es el plazo de conservación de los datos personales?	7 años.
--	---------

12 Buzón de quejas y sugerencias	
<i>Finalidad del tratamiento</i>	Los datos personales que nos proporcione de manera presencial, por escrito, vía correo electrónico, por teléfono y mediante formulario de Google en la web, serán utilizados con fines de registro, seguimiento, respuesta a las quejas, sugerencias, control e informes sobre las peticiones atendidas.
<i>Datos personales recabados</i>	Nombre completo, número telefónico y correo electrónico. No se recaban Datos Personales Sensibles.
¿Cómo se obtienen los datos personales?	Directamente del titular, con la presencia física, vía telefónica, correo electrónico y sistemas informáticos.
<i>Uso de los datos</i>	Con fines de registro, seguimiento, respuesta a las quejas, sugerencias, control e informes sobre las peticiones atendidas.
<i>Formato de almacenamiento</i>	Físico y Electrónico (Base de datos en formatos Excel).
<i>Descripción general de la ubicación física y/o electrónica de los datos personales</i>	Carpeta compartida en el Departamento de Departamento de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Contraloría Social en los servidores del SEECAT, únicamente personal facultado por la Coordinación General cuenta con acceso a dicha carpeta.
<i>Fundamento legal</i>	Artículo 3, fracciones X, XI y XXXIV, 11, 29 fracción VI, 130 fracción II y 131 de la LPDPPSOEQROO.
<i>Cargo del servidor público responsable</i>	Jefe de Departamento de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Contraloría Social
<i>Servidores públicos que tienen acceso a los sistemas de tratamiento</i>	Coordinador General del SEECAT, jefes de departamento de todas las áreas del SEECAT.
¿Intervienen encargados en el tratamiento de datos personales?	No.
¿Se realizan transferencias de datos personales y con qué finalidad?	Se informa que no se realizarán transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
¿Cuál es el plazo de conservación de los datos personales?	7 años

13 Supervisiones a participantes del Programa de Apoyo al Empleo	
<i>Finalidad del tratamiento</i>	Los datos personales que proporcione de manera presencial y por escrito mediante los formatos de supervisión, serán utilizados con fines de registro, seguimiento y control e informes sobre las supervisiones realizadas a procesos del Programa de Apoyo al Empleo, y/o programas complementarios tales como Capacítate y Empléate.
<i>Datos personales recabados</i>	Nombre completo, firma autógrafa. No se recaban Datos Personales Sensibles.

¿Cómo se obtienen los datos personales?	Directamente del titular, con la presencia física.
Uso de los datos	Con fines de registro, seguimiento y control e informes sobre las supervisiones realizadas a procesos del Programa de Apoyo al Empleo.
Formato de almacenamiento	Físico y Electrónico (Base de datos en formatos Excel).
Descripción general de la ubicación física y/o electrónica de los datos personales	Carpeta compartida en el Departamento de Departamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales en los servidores del SEECAT, únicamente personal facultado por la Coordinación General cuenta con acceso a dicha carpeta.
Fundamento legal	Artículo 3, fracciones X, XI y XXXIV, 11, de la LPDPPSOEQROO.
Cargo del servidor público responsable	Jefe de Departamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.
Servidores públicos que tienen acceso a los sistemas de tratamiento	Coordinador General del SEECAT, jefes de departamento de todas las áreas del SEECAT.
¿Intervienen encargados en el tratamiento de datos personales?	No.
¿Se realizan transferencias de datos personales y con qué finalidad?	Se informa que no se realizarán transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
¿Cuál es el plazo de conservación de los datos personales?	7 años

14 Lista de atendidos del Programa de Apoyo al Empleo

Finalidad del tratamiento	Los datos personales que proporcione a través de la Lista de Atendidos, serán utilizados con fines de registro y control de personas atendidas por alguno de los Subprogramas del Programa de Apoyo al Empleo.
Datos personales recabados	Nombre completo, teléfono, correo electrónico y firma autógrafa. No se recaban Datos Personales Sensibles.
¿Cómo se obtienen los datos personales?	Directamente del titular, con la presencia física.
Uso de los datos	Con fines de registro y control de personas atendidas por alguno de los Subprogramas del Programa de Apoyo al Empleo.
Formato de almacenamiento	Físico y Electrónico (Base de datos en formatos Excel).
Descripción general de la ubicación física y/o electrónica de los datos personales	Carpeta compartida en el Departamento de Departamento de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Contraloría Social en los servidores del SEECAT, únicamente personal facultado por la Coordinación General cuenta con acceso a dicha carpeta.
Fundamento legal	Artículo 3, fracciones X, XI y XXXIV, 11 de la LPDPPSOEQROO

<i>Cargo del servidor público responsable</i>	Jefe de Departamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.
<i>Servidores públicos que tienen acceso a los sistemas de tratamiento</i>	<i>Coordinador General del SEECAT, jefes de departamento de todas las áreas del SEECAT.</i>
¿Intervienen encargados en el tratamiento de datos personales?	No.
¿Se realizan transferencias de datos personales y con qué finalidad?	Se informa que no se realizarán transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
¿Cuál es el plazo de conservación de los datos personales?	7 años

15 Eventos públicos	
<i>Finalidad del tratamiento</i>	Los datos personales que nos proporcione de manera presencial o virtual, así como imágenes en fotografías y videos serán utilizados con fines de llevar un control de participantes, dar a conocer las actividades institucionales y difusión de estas en los medios de comunicación y redes sociales.
<i>Datos personales recabados</i>	Nombre completo, sexo, género, imagen (video o captura), correo electrónico. No se recaban Datos Personales Sensibles.
¿Cómo se obtienen los datos personales?	Videos y grabaciones en eventos públicos.
<i>Uso de los datos</i>	Con fines de llevar un control de personas atendidas por alguno de los Subprogramas del Programa de Apoyo al Empleo; difundir y dar a conocer las actividades institucionales en los medios de comunicación y redes sociales.
<i>Formato de almacenamiento</i>	Electrónico audio y video.
<i>Descripción general de la ubicación física y/o electrónica de los datos personales</i>	Carpeta de imágenes y audio en el Departamento de Vinculación Laboral, únicamente personal facultado por la Coordinación General cuenta con acceso a dicha carpeta.
<i>Fundamento legal</i>	Artículo 3, fracciones X, XI y XXXIV, 11 de la LPDPPSOEQROO
<i>Cargo del servidor público responsable</i>	Jefe de Departamento de Vinculación Laboral
<i>Servidores públicos que tienen acceso a los sistemas de tratamiento</i>	<i>Coordinador General del SEECAT, jefes de departamento de todas las áreas del SEECAT.</i>
¿Intervienen encargados en el tratamiento de datos personales?	No.
¿Se realizan transferencias de datos personales y con qué finalidad?	Se informa que no se realizarán transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.

¿Cuál es el plazo de conservación de los datos personales?

7 años

ANEXO 2. Metodología de la gestión de riesgos del SEECAT

Valoración de los activos.

Se valoró cuantitativa y cualitativamente cada dimensión de seguridad. La escala de valor para cada propiedad será de 1 a 3, donde 1 es bajo, 2 es medio y 3 es alto, una vez determinados los valores individuales, se sumarán para obtener el valor total del activo, donde:

Valor cuantitativo	Valor cualitativo
1-3	Bajo
4-6	Medio
7-9	Alto

No.	Nombre del activo	PRINCIPIOS DE SEGURIDAD			VALOR DEL ACTIVO	
		Confidencialidad	Integridad	Disponibilidad	Cualitativo	Cuantitativo
1	Expedientes físicos del personal del SEECAT.	1	1	1	3	Bajo
2	Expedientes físicos de buscadores de empleo y empleadores	3	3	3	9	Alto
3	Sistema de Intermediación Laboral para la Atención Personalizada	2	2	2	6	Medio
4	Sistema Informático de Movilidad Laboral	2	2	2	6	Medio

Criterios de Probabilidad

Se refiere a la posibilidad de que un evento ocurra, considerando la cantidad de veces que podría presentarse en determinado periodo de tiempo, basándose en las eventualidades conocidas y el conocimiento del entorno.

Grado de probabilidad		Criterio
Baja	1	Si ha ocurrido 1 antecedente registrado en un periodo de 5 años o y/o que, por el entorno, la posibilidad de que suceda sea mínima.
Media	2	Si solo se han tenido 2 antecedentes registrado en un periodo anual y/o esporádicamente en un intervalo de 3 años, o que por el tipo de entorno y condiciones sea posible que ocurra.
Alta	3	Si ha habido más de dos eventos al término de un año o bien que por las condiciones actuales o el tipo de entorno sea sumamente posible que suceda.

Activo	Amenaza	Probabilidad	
		Cuantitativa	Cualitativa
Expedientes físicos del personal del SEECAT.	Robo de información	1, no existe antecedente y es poco probable que ocurra.	Baja
Expedientes físicos del personal del SEECAT.	Incendio	1, no existe antecedente y es poco probable que ocurra.	Baja
Expedientes físicos de buscadores de empleo y empleadores	Robo de información	1, no existe antecedente y es poco probable que ocurra.	Baja
Expedientes físicos de buscadores de empleo y empleadores	Incendio	1, no existe antecedente y es poco probable que ocurra.	Baja
Sistema de Intermediación Laboral para la Atención Personalizada	Robo de información	1, no existe antecedente y es poco probable que ocurra.	Baja
Sistema Informático de Movilidad Laboral	Robo de información	1, ha ocurrido 1 antecedente registrado en un periodo de 5 años.	Baja

Impacto:

Medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización.

El impacto deberá valorarse en una escala cualitativa y una cuantitativa y en las tres dimensiones de seguridad (en la confidencialidad, en la integridad y en la disponibilidad) se recomienda de 1 a 3, donde 1 es bajo, 2 es medio y 3 es alto.

Valor objetivo	Valor subjetivo
1	Bajo
2	Medio
3	Alto

Debemos considerar que el impacto debe analizarse por cuanto, a los daños o afectaciones a las personas titulares de datos personales, y no así la afectación a la organización, particularmente a su reputación, que, si bien importa y afecta, no es el fin último y propósito del Documento de Seguridad, en tanto que se trata de la protección de un derecho fundamental.

Activo	Amenaza	Impacto			Impacto total	
		Confidencialidad	Integridad	Disponibilidad	Valor cuantitativo	Valor cualitativo
Expedientes físicos del personal del SEECAT.	Robo de información	2	2	1	1.6=2	Medio
Análisis del impacto en los titulares: De materializarse el riesgo "Robo de información", los peores escenarios que pudieran observarse para los titulares son: • Daños en su integridad y seguridad dado que el expediente contiene su dirección, CURP y teléfono particular. • Pérdida de control de sus datos personales. • Problemas jurídicos en caso de que se modifiquen los datos sobre su historia académica o experiencia laboral.						
Expedientes físicos del personal del SEECAT.	Incendio	1	1	1	1	Bajo
Análisis del impacto en los titulares: De materializarse el riesgo "Incendio", no se considera que haya un impacto directo sobre los titulares, salvo causa de molestias en caso de tener que solicitarlos nuevamente.						

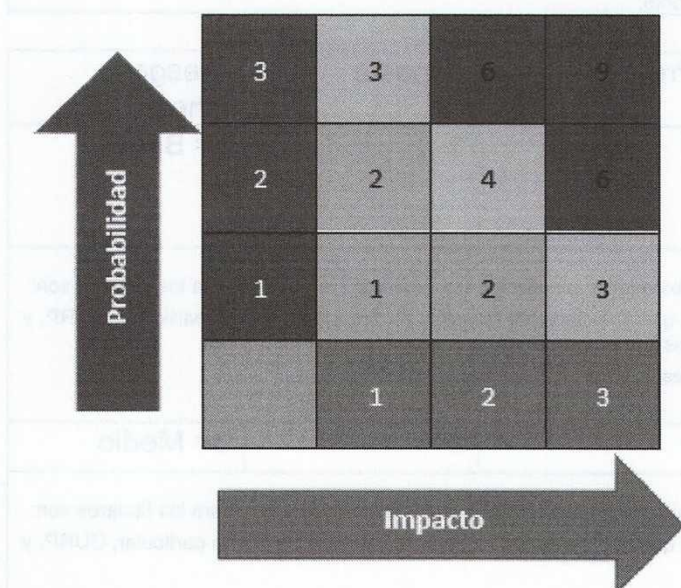
Activo	Amenaza	Impacto			Impacto total	
		Confidencialidad	Integridad	Disponibilidad	Valor cuantitativo	Valor cualitativo
Expedientes físicos de buscadores de empleo y empleadores	Robo de información	2	2	1	1.6=2	Medio
Análisis del impacto en los titulares: De materializarse el riesgo "Robo de información", los peores escenarios que pudieran observarse para los titulares son: • Daños en su integridad y seguridad dado que el expediente contiene su dirección, teléfono particular, CURP, y alta ante el IMSS (en caso de empleadores). • Pérdida de control de sus datos personales.						
Expedientes físicos de buscadores de empleo y empleadores	Incendio	1	1	1	1	Bajo
Análisis del impacto en los titulares: De materializarse el riesgo "Incendio", no se considera que haya un impacto directo sobre los titulares, salvo causa de molestias en caso de tener que solicitarlos nuevamente.						

Activo	Amenaza	Impacto			Impacto total	
		Confidencialidad	Integridad	Disponibilidad	Valor cuantitativo	Valor cualitativo
Sistema de Intermediación Laboral para la Atención Personalizada	Robo de información	2	1	1	1.3=1	Bajo
Análisis del impacto en los titulares: De materializarse el riesgo "Robo de información", los peores escenarios que pudieran observarse para los titulares son: • Daños en su integridad y seguridad dado que el expediente contiene su dirección, teléfono particular, CURP, y alta ante el IMSS (en caso de empleadores). • Pérdida de control de sus datos personales.						
Sistema Informático de Movilidad Laboral	Robo de información	3	3	2	2.6=3	Alto
Análisis del impacto en los titulares: De materializarse el riesgo "Robo de información", los peores escenarios que pudieran observarse para los titulares son: • Daños en su integridad y seguridad dado que el expediente contiene su dirección, teléfono particular, CURP, y montos de ingresos anuales. • Pérdida de control de sus datos personales. • Usurpación de identidad						

Valoración del riesgo inherente:

Riesgo= probabilidad x impacto

Teniendo valores cualitativos y cuantitativos podemos valorar el riesgo, para ello podemos utilizar una matriz de riesgo o un mapa de calor, como el siguiente ejemplo:



Donde:

1-2= Riesgo bajo

3-5= Riesgo medio

6-9= Riesgo alto

Así calculamos el riesgo intrínseco o inherente.

Activo	Amenaza	Probabilidad	Impacto	Riesgo inherente
Expedientes físicos del personal del SEECAT.	Robo de información	1	2	2= Bajo
Análisis del impacto en los titulares: De materializarse el riesgo "Robo de información", los peores escenarios que pudieran observarse para los titulares son: • Daños en su integridad y seguridad dado que el expediente contiene su dirección, CURP y teléfono particular. • Pérdida de control de sus datos personales. • Problemas jurídicos en caso de que se modifiquen los datos sobre su historia académica o experiencia laboral.				
Expedientes físicos del personal del SEECAT.	Incendio	1	1	1=Bajo
Análisis del impacto en los titulares: De materializarse el riesgo "Incendio", no se considera que haya un impacto directo sobre los titulares, salvo causa de molestias en caso de tener que solicitarlos nuevamente.				

Activo	Amenaza	Probabilidad	Impacto	Riesgo inherente
Expedientes físicos de buscadores de empleo y empleadores	Robo de información	1	2	2= Bajo
Análisis del impacto en los titulares: De materializarse el riesgo "Robo de información", los peores escenarios que pudieran observarse para los titulares son: • Daños en su integridad y seguridad dado que el expediente contiene su dirección, CURP y teléfono particular. • Pérdida de control de sus datos personales. • Problemas jurídicos en caso de que se modifiquen los datos sobre su historia académica o experiencia laboral.				
Expedientes físicos de buscadores de empleo y empleadores	Incendio	1	1	1= Bajo
Análisis del impacto en los titulares: De materializarse el riesgo "Incendio", no se considera que haya un impacto directo sobre los titulares, salvo causa de molestias en caso de tener que solicitarlos nuevamente.				

Activo	Amenaza	Probabilidad	Impacto	Riesgo inherente
Sistema de Intermediación Laboral para la Atención Personalizada	Robo de información	1	1	1= Bajo
Análisis del impacto en los titulares: De materializarse el riesgo "Robo de información", los peores escenarios que pudieran observarse para los titulares son: • Daños en su integridad y seguridad dado que el expediente contiene su dirección, teléfono particular, CURP, y alta ante el IMSS (en caso de empleadores). • Pérdida de control de sus datos personales.				
Sistema Informático de Movilidad Laboral	Robo de información	1	3	3= Medio
Análisis del impacto en los titulares: De materializarse el riesgo "Robo de información", los peores escenarios que pudieran observarse para los titulares son: • Daños en su integridad y seguridad dado que el expediente contiene su dirección, teléfono particular, CURP, y montos de ingresos anuales. • Pérdida de control de sus datos personales.				

- Usurpación de identidad

ANEXO 3. Análisis de brecha

Un análisis de brecha es una comparación de las medidas de seguridad existentes en una empresa u organización contra las que sería conveniente tener, a fin de establecer un plan de trabajo para completar las medidas de seguridad faltantes.

El SEECAT ha considerado poner en marcha medidas de seguridad básicas para minimizar las vulneraciones a la seguridad de los datos personales y sistemas de tratamiento; bajo las siguientes categorías generales:

- A) Medidas de seguridad basadas en la cultura del personal.
- B) Medidas de seguridad en el entorno de trabajo físico.
- C) Medidas de seguridad en el entorno de trabajo digital.

Explicación de cada una de las categorías generales:

A. Medidas de seguridad basadas en la cultura del personal

Una de las principales causas por las que ocurre robo o extravío de datos personales e incluso de cualquier información relevante para la organización, es simplemente porque los datos no se cuidan adecuadamente. El siguiente grupo de preguntas tienen como objetivo identificar las prácticas inadecuadas más comunes, que podrían provocar una vulneración a la seguridad.

A.1. **¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?**

Cuando se dejan datos personales sin supervisión o por descuido, éstos corren el riesgo de ser sustraídos por alguien más (interno o externo a la organización). Por ello es importante considerar controles como:

A.1.1. Política de escritorio limpio: No dejar a simple vista documentos importantes, equipo de cómputo, contraseñas en "post-it", llaves, identificaciones, entre otros.

A.1.2. Hábitos de cierre y resguardo: Esto debe incluir conductas como: que cada empleado cierre sus cajones, que las cosas importantes siempre se mantengan bajo llave si no están en uso y/o que el último en salir de las oficinas cierre los archiveros y las puertas con llave, y active las alarmas en su caso.

A.1.3. Impresoras, escáneres, copiadoras y buzones limpios: Nunca se deben dejar abandonados documentos en áreas de uso común como las ya mencionadas.

A.1.4. Gestión de bitácoras, usuarios y acceso: Para controlar el acceso a los sitios, medios de almacenamiento, formatos y equipo de cómputo, se puede hacer con bitácoras tan simples como una lista donde se anote el nombre, fecha y hora de la

persona que accede a un archivero para consultar un expediente, o bien, llevar bitácoras automatizadas para el uso de medios electrónicos. Es importante habilitar los mecanismos de registro en los equipos de cómputo y su software para identificar la actividad de los usuarios. Así como revisar que las credenciales y permisos de los usuarios estén bien definidos.

A.2. ¿Tienes mecanismos para eliminar de manera segura la información?

Si cualquier documento es depositado simplemente en la basura, éste puede ser recuperado y visto por cualquier persona malintencionada, y así ocurrir una fuga de información importante. Por otra parte, en los medios electrónicos, la simple acción de "borrado" no elimina de forma definitiva la información, y ésta puede ser recuperada desde los dispositivos desechados, con ciertas herramientas. Por ello se deben tomar en cuenta controles como:

A.2.1. Destrucción segura de documentos: Los documentos y otros medios físicos no deben simplemente desecharse una vez que ya no se utilizan, sino destruirse por ejemplo con triturado o incinerado. Cuando se adquiere equipo para estas tareas se debe evaluar que tan difícil sería para una persona recuperar la información, por ejemplo, hay trituradoras que hacen tiras el papel y otras que lo hacen pequeños trozos. Con tiempo y esfuerzo es posible recuperar un documento hecho tiras, pero es muy difícil recuperar uno hecho "confeti" o cenizas. Otra opción es almacenar en un sitio seguro los documentos a triturar y entregarlos periódicamente a alguien que preste el servicio de destrucción de documentos, sin olvidar que debe existir un contrato que estipule claramente el deber de confidencialidad del prestador de servicio.

A.2.2. Destrucción segura de información en equipo de cómputo y medios de almacenamiento electrónico: Es conocido que en los equipos de cómputo se puede "borrar" o "eliminar" la información de forma simple o con un clic, pero debido a la naturaleza del almacenamiento electrónico, lo que ocurre en realidad, es que ésta deja de ser fácilmente accesible, pero sigue ahí hasta que nueva información la "sobrescribe". Para la eliminación definitiva de información existen herramientas de software que borran archivos electrónicos específicos o dispositivos de almacenamiento completos. Cuando la vida útil de un equipo de cómputo o medio de almacenamiento electrónico ha terminado, es recomendable destruirlo físicamente. Esto lo puede hacer la misma organización o contratar a un tercero para este servicio, cuando la cantidad de equipo de cómputo es mayor.

A.2.3. Fijar periodos de retención y destrucción de información: Es importante identificar de manera regular toda la información que ya no es de utilidad para la organización y que no requiere almacenarse para cumplir con alguna responsabilidad legal o contractual. Los procedimientos de eliminación de información de gran valor o a gran escala deben ser formales y se deben registrar en bitácoras.

A.2.4. Tomar precauciones con los procedimientos de re-utilización: Por diversas razones, las organizaciones pueden optar por diferentes mecanismos de reciclado para minimizar costos, pero se debe ser cuidadoso en la posible exposición de datos personales. Por ejemplo, es común el uso de "bandejas de papel reciclado", pero bajo ninguna circunstancia deberían utilizarse documentos con datos personales como "papel de reúso". Cuando el equipo de cómputo tenga que cambiar de dueño, por

ejemplo, de un empleado a otro, es importante respaldar la información relevante para la organización y borrar completamente los datos que resguarda el equipo.

A.3. ¿Has establecido y documentado los compromisos respecto a la protección de datos?

Todos aquellos involucrados en el tratamiento de datos personales deben actuar con relación a los principios que establece la Ley. No se deben obviar o dejar como reglas implícitas todas aquellas relacionadas a la privacidad y protección de datos personales de las personas. De manera adicional, se debe fomentar la cultura de la seguridad y la noción del valor intrínseco de la información. Por ello, se deben considerar estrategias como:

A.3.1. Informar al personal sobre sus deberes mínimos de seguridad y protección de datos:

El personal involucrado en el tratamiento de datos personales debe estar informado de manera explícita que tiene un compromiso y responsabilidad sobre la información en su custodia, y en su caso tareas específicas a realizar. Esto incluye, por ejemplo, informar al personal de nuevo ingreso sobre sus funciones y obligaciones para la protección de datos e incluir cláusulas al respecto cuando se hace una contratación. En su caso, también se debe informar a los empleados de las posibles consecuencias y medidas disciplinarias relacionadas, en caso de no cumplir con sus deberes.

A.3.2. Fomentar la cultura de la seguridad de la información: En el trabajo diario, es común que a todas las personas que manejan información personal de manera continua, se les vuelva una actividad rutinaria, esto puede provocar que sean descuidados con la gestión de la información. Por lo que es necesario permear la seguridad de la información como una práctica cotidiana, recordando la importancia de este deber e incentivando a los empleados, para que entre ellos se recuerden el uso de medidas de seguridad y buenos hábitos de tratamiento.

A.3.3. Difundir noticias en temas de seguridad: Mantener informado al personal respecto a las últimas noticias en seguridad puede parecer complejo, sin embargo, existen muchos medios de comunicación, como las redes sociales, por los cuales las organizaciones se pueden mantener al tanto de las historias más relevantes en seguridad.

A.3.4. Prevenir al personal sobre la Ingeniería Social: De manera general se considera a la ingeniería social como un conjunto de técnicas para influenciar a una persona a tomar acciones que pueden estar o no dentro de sus intereses o responsabilidades. Estas técnicas pueden ser utilizadas por criminales para engañar a personas desprevenidas en línea, por teléfono o personalmente. Se debe invitar al empleado a que sea "cauto y cortés" es decir, que se cuestione en todo momento si alguna solicitud tiene sentido y si está dentro de sus responsabilidades cumplirla, de lo contrario negarse educadamente a entregar la información o a realizar la acción solicitada e informar de este hecho a su jefe inmediato.

A.3.5. Asegurar la protección de datos personales en subcontrataciones: La organización no debe asumir que un proveedor o cualquier externo tomará las medidas de seguridad necesarias para proteger la información personal y que la tratará como

confidencial, sin que esto se manifieste explícitamente. Por ejemplo, a través de cláusulas que especifiquen claramente el tratamiento legítimo y las medidas de seguridad implementadas para la protección de los datos personales. Otros tipos de convenio que deben revisarse son los relacionados a la compra, venta o intercambio de datos de titulares, revisando a detalle que los datos sean utilizados con el consentimiento del titular. Además, en el uso de servicios de almacenamiento en línea o de cómputo en la nube, por ejemplo, el correo electrónico, se debe revisar y evaluar si el contrato de adhesión garantiza seguridad y confidencialidad de los datos que se almacenen.

A.4. ¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?

Para las organizaciones, incluso para aquéllas con gran madurez en el tema de seguridad de la información, el tema de vulneraciones a la seguridad de los datos personales puede resultar particularmente complicado, la idea básica es disminuir la afectación a los titulares de los datos personales y a la organización. Por eso, se requiere tomar medidas como:

A.4.1. Tener un procedimiento de notificación: Se debe tener establecida una cadena de avisos dentro de la empresa u organización en caso de que ocurra una vulneración a la seguridad. Cuando un empleado sufra o identifique un incidente de seguridad, éste debe tener muy claro a quién debe avisar en la empresa u organización. El responsable debe evaluar qué información se afectó y los medios para notificar a los titulares de lo ocurrido, esto con el fin de alertarlos y que tomen precauciones. Adicionalmente, se podrá diagnosticar el posible impacto a las operaciones y tomar acciones que mitiguen el incidente, por ejemplo, actualizando sus procedimientos y medidas de seguridad.

A.4.2. Realizar revisiones y auditorías: Se debe considerar la revisión periódica a la empresa u organización por un especialista en temas de seguridad para que éste realice evaluaciones y recomendaciones. Por la naturaleza técnica de algunas amenazas, este tipo de revisiones podrían ayudar a revelar malas prácticas en el tratamiento de datos personales o la existencia de vulneraciones a la seguridad no detectadas, por ejemplo, a través de las llamadas pruebas de penetración o pentest. Los resultados de cualquier evaluación deben informarse a los empleados involucrados en el tratamiento de datos personales.

El Reglamento de la Ley establece que el responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado acciones para reducir la posible afectación a los titulares. La notificación a los titulares debe considerar al menos:

- La naturaleza de la vulneración
- Los datos personales comprometidos del titular
- Recomendaciones al titular para proteger sus intereses
- Las acciones correctivas realizadas de forma inmediata

- Los medios donde puede obtener más información al respecto

A.5. ¿Realizas respaldos periódicos de los datos personales?

En la medida de lo posible se deben almacenar los documentos físicos en medio electrónico, es decir, capturar, digitalizar o escanear la información en papel para almacenarla, de forma tal que se resguarde el mínimo de información en papel y sólo se imprima cuando sea estrictamente necesario. Esto debido a que es más práctico respaldar información copiando un archivo de un medio electrónico a otro, comparado con fotocopiar, organizar y almacenar documentos en papel. Los datos personales almacenados en equipo de cómputo pueden dañarse de manera parcial o total debido a fallas en los sistemas o aplicaciones, por errores de operación de las personas, o bien por interrupciones de energía eléctrica, si se realizan respaldos de la información importante de manera periódica pueden mitigarse las consecuencias de estos incidentes. Es importante que los respaldos se realicen de manera regular y también cada vez que haya una actualización importante de los datos que están siendo almacenados en la organización. Se pueden realizar respaldos parciales sólo de la información crítica, diario o cada semana, y respaldos de toda la información, cada quince días o mensualmente. Es importante que los respaldos no se encuentren en la misma ubicación física que la información que se están respaldando y hacer pruebas de recuperación de las copias de respaldo para asegurarnos de que la información se encuentra íntegra.

B. Medidas de seguridad en el entorno de trabajo físico

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.

B.1. ¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?

El acceso al entorno de trabajo físico debe ser sólo para personal autorizado, si no existen restricciones para el acceso, se corre el riesgo de que los datos personales sean robados o manipulados. De manera particular, ninguna persona sin autorización debería poder acercarse al equipo de cómputo, archiveros con datos personales, o a cualquier otro medio de almacenamiento. Para esto se deben considerar medidas como:

B.1.1. Alerta del entorno de trabajo: No se debe permitir que alguien sin motivos relacionados al funcionamiento del negocio ingrese al entorno de trabajo. Se debe tener precaución con las personas no autorizadas al entorno, por ejemplo, en las oficinas de la empresa u organización debería haber áreas como un mostrador de recepción o si se está trabajando en un café se debería evitar que alguna persona extraña esté muy cerca de los elementos donde se tengan datos personales. Siempre se debe cuestionar la presencia de un extraño sin acompañamiento o que se encuentre cerca del entorno de trabajo.

B.1.2. Mantener bitácoras del personal con acceso al entorno de trabajo: En entornos como oficinas es importante mantener un registro de todos los que ingresan

y salen y acordar que aquéllos que salen al final del entorno de trabajo deben poner especial atención, dicho de manera coloquial el “último en salir cierra”.

B.2. ¿Tienes medidas de seguridad para evitar el robo?

Se deben establecer medidas con las cuales se minimice el riesgo de que alguien robe información fácilmente. Por ejemplo:

B.2.1. Cerraduras y candados: En las oficinas de la empresa u organización o en casa se debe contar como mínimo con gavetas, escritorios, o archiveros que se puedan cerrar con llave. El mismo principio aplica para otros entornos, usando candados para laptops o maletas con cierre de combinación.

B.2.2. Elementos disuasorios: Existen medidas de seguridad que reducen de manera significativa el interés de un atacante, por ejemplo, alarmas (tanto para el entorno como para los dispositivos), guardias de seguridad, rejas, maletines de seguridad, entre otros.

B.2.3. Minimizar el riesgo oportunista: Es necesario limitar el número de entornos de trabajo donde se realice tratamiento de datos personales (por ejemplo, sólo en casa o en la oficina), si es necesario trabajar constantemente en otros entornos (como aeropuertos u oficinas de otros clientes) se debe permanecer especialmente cauto del entorno y nunca dejar un elemento con datos personales sin supervisión.

B.3. ¿Cuidas el movimiento de información en entornos de trabajo físicos?

Al realizar envío de información siempre se corre el riesgo de que ésta se pierda o sea robada. Por ello, es importante tener controles de seguridad que minimicen el impacto del extravío, como:

B.3.1. Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico: Se debe registrar el permiso o la acción relacionada a la salida de los elementos mencionados en una bitácora, esto con el fin de que, en caso de pérdida, robo, daño o extravío se tenga control del posible impacto.

B.3.2. Mantener en movimiento sólo copias de la información, no el elemento original: Un incidente común en las organizaciones de cualquier tamaño es que la información que se pierde es la única información disponible. La información que sale de los entornos de trabajo usuales debería ser una copia, y no la información original.

B.3.3. Usar mensajería certificada: Es importante que el envío físico de medios que contienen datos personales se realice con mensajería segura/certificada, o en su defecto con personal de confianza, y siempre se debe recabar el acuse de recibo del envío.

C. Medidas de seguridad en el entorno de trabajo digital

Muchas de las operaciones de las organizaciones y de los mismos titulares 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).

C.1. ¿Realizas actualizaciones al equipo de cómputo?

Si una deficiencia en la seguridad de un equipo de cómputo (llamada vulnerabilidad o agujero) no es atendida, el equipo puede infectarse con malware o tener algún malfuncionamiento. Los productos de software como sistemas operativos, programas y aplicaciones deben encontrarse en sus versiones más recientes y/o debidamente actualizadas. La mayoría del equipo de cómputo de uso común y su software está configurado para actualizarse de manera periódica, sin embargo, debe verificarse que efectivamente esté habilitada esta funcionalidad, de lo contrario se debe programar al menos una vez al mes un espacio para realizar las actualizaciones correspondientes.

C.2. ¿Revisas periódicamente el software instalado en el equipo de cómputo?

Es importante revisar periódicamente qué tipos de programas se encuentran instalados en el equipo de cómputo, para verificar que se esté utilizando sólo software autorizado y evitar la instalación de software no deseado. Es de especial importancia evitar el uso de software para “bajar” o compartir archivos en equipos de cómputo de la organización, o con otros dispositivos personales, como tabletas o celulares, no sólo para evitar infringir la ley de derechos de autor, sino porque este software puede dar acceso a la información de un equipo a personas malintencionadas. También se debe vigilar que no se tenga instalado software sin licencia o “pirata”, ya que éste podría estar infectado o simplemente no operar como el original y causar pérdida de información.

C.3. ¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?

El equipo de cómputo es susceptible a que cualquiera lo pueda utilizar, incluso personal no autorizado. Se deben tomar medidas de seguridad para evitar que alguien use un equipo de cómputo, medio de almacenamiento electrónico o acceda a un entorno de trabajo digital sin autorización, por ejemplo, mediante el uso de contraseñas y/o cifrado, o de aplicaciones o dispositivos para la verificación de identidad del usuario.

C.3.1. Uso de contraseñas y/o cifrado: Toda información personal en medio digital debería estar protegida con bloqueos por contraseña y/o cifrado, para evitar su acceso no autorizado y posibles eventos de robo o pérdida de información.

C.3.2. Uso de contraseñas sólidas: Una contraseña débil es susceptible a ser “crackeada” es decir, averiguar la contraseña con herramientas de software o simplemente adivinando. Se debe evitar el uso de información personal o palabras simples en las contraseñas. Aunque es una recomendación usual el crear contraseñas mezclando caracteres especiales y números para hacerlas difícil de adivinar, también puede ser difícil para los usuarios memorizarlas, y provocar que recaigan en malas prácticas como tenerlas escritas a la vista. Una mejor alternativa puede ser el uso de “passphrases”, es decir, frases o ideas completas, por ejemplo, “me gusta la pizza de jamón”, esta es una contraseña segura por ser muy larga y difícil de adivinar, pero es fácil de aprender. Otra opción es usar software de administración de contraseñas.

C.3.3. Bloqueo y cierre de sesiones: Cuando no se utilice el equipo de cómputo se debe bloquear o cerrar la sesión de usuario. Si un equipo no se va a utilizar por un periodo largo, se debe optar por apagarlo. Todo inicio de sesión debe requerir el uso de una contraseña, token, u otro mecanismo de autenticación. También se pueden considerar mecanismos de bloqueo y borrado remoto para los dispositivos móviles, de forma tal que se pueda restringir o eliminar la información aun cuando un equipo haya sido robado o extraviado.

C.3.4. Administrar usuarios y accesos: Se debe minimizar el uso de credenciales compartidas, es decir, que más de una persona tenga acceso al mismo servicio con el mismo usuario y contraseña, por ejemplo, que dos personas distintas usen la misma identificación para usar la misma cuenta de correo. En su caso, cuando se implementan sistemas de tratamiento más complejos, por ejemplo, bases de datos, se debe tener una correcta administración de los usuarios, contraseñas y privilegios de acceso (permisos para leer y modificar un archivo).

C.4. ¿Revisas la configuración de seguridad del equipo de cómputo?

El equipo de cómputo, el software y en algunas ocasiones los medios de almacenamiento electrónico tienen configuraciones que permiten incrementar su nivel de seguridad. Los responsables deben habilitar las opciones de seguridad que permita a sus equipos estar más seguros, por ejemplo, encender el firewall o habilitar las actualizaciones automáticas del antivirus, esta práctica, conocida como hardening o endurecimiento, puede requerir de cierto estudio y dedicación. Sin embargo, gracias a lo amigable de las nuevas herramientas, así como a la información disponible en los sitios de Internet para soporte en línea del fabricante o proveedor, esta tarea es más fácil y podemos incrementar el nivel de seguridad significativamente. Es conveniente que todos los equipos de la organización, ya sean fijos o portátiles, mantengan un mismo nivel de configuración de seguridad.

C.5. ¿Tienes medidas de seguridad para navegar en entornos digitales?

El uso cotidiano de los equipos de cómputo y de los entornos digitales hace que se den por obvias algunas conductas que podrían representar riesgo a los datos personales, por ello se deben implementar medidas de seguridad como:

C.5.1. Instalar herramientas antimalware y de filtrado de tráfico: el software malicioso o malware comprende diferentes tipos como virus, troyanos, gusanos, entre otros, que tiene por objetivo extraer datos de los usuarios como sus contraseñas o números de cuenta bancaria. Se debe instalar al menos, software antivirus y habilitar el filtrado de tráfico (como un firewall).

C.5.2. Reglas de navegación segura: Sólo se deben revisar sitios web esenciales para el negocio, evitando navegar en sitios no relacionados y mucho menos en sitios de riesgo como son los de descarga de contenido que violan los derechos de autor o pornográficos. Todos los empleados deben estar informados de los riesgos a los que se exponen por visitar sitios web que no son relevantes para sus funciones, también se les debe informar del peligro relacionado a la descarga de contenido, y la ventaja de verificar que el protocolo de conexión a los sitios web sea seguro, es decir, verificar que en la dirección web aparezca https y la imagen de un candado, en lugar de que sólo

sea http. Además, se puede optar por herramientas de cifrado de las comunicaciones como las redes virtuales privadas (o VPN, Virtual Private Network).

C.5.3. Reglas para la divulgación de información: Antes de enviar información a un tercero, almacenarla en cuentas de cómputo en la nube, publicarla en un sitio web, o compartirla en redes sociales, se debe evaluar si esta acción no está poniendo en riesgo a titulares o a personal de la organización.

C.5.4. Uso de conexiones seguras: Además de verificar que los protocolos de navegación sean seguros, se debe cuidar que la conexión también sea confiable. Cuando se trate de redes inalámbricas, éstas deberán contar con contraseñas y configuración segura (por ejemplo, WPA o WPA2, evitando conectarse o configurar redes WEP o abiertas, susceptibles a que un externo malintencionado intercepte las comunicaciones).

Asimismo, es preferible evitar el uso de redes públicas, particularmente en los casos en que sea necesario llevar a cabo una transacción que implique el uso de información personal o contraseñas (por ejemplo, acceder a un portal bancario mediante un dispositivo portátil, utilizando una red WiFi provista por un sitio público, como un aeropuerto o una cafetería). De manera general, si no se puede asegurar la conexión, se deberá evitar cualquier tratamiento que involucre datos personales en línea.

C.6. ¿Cuidas el movimiento de información en entornos de trabajo digitales?

El envío erróneo o interceptación de mensajes electrónicos (ya sea correo, mensajería instantánea, redes sociales, mensajes de texto a celular, entre otros) representa una grave fuga de información que puede perjudicar seriamente a los titulares. Es por esto que se debe considerar:

C.6.1. Validación del destinatario de una comunicación: Se han registrado muchos incidentes en los cuales la información personal se ha fugado a terceros debido a la transmisión errónea de mensajes electrónicos como correos, faxes, redes sociales, entre otros. Antes de enviar un mensaje se debe asegurar que el envío se realiza al destinatario correcto. Cuando se envíe un mensaje electrónico a varios destinatarios se debe revisar el método de envío y designación (por ejemplo, en correo electrónico, CC o con copia, CCO o con copia oculta).

C.6.2. Seguridad de la información enviada y recibida: Cuando se envía información importante a través de mensajes electrónicos, ésta no se debería incluir bajo ninguna circunstancia en el cuerpo del mensaje, sino en un archivo individual protegido por contraseña/cifrado, la contraseña no debe estar contenida en el cuerpo del mensaje del que se envía la información, sino en un mensaje distinto o comunicarse por otro medio (por ejemplo, por teléfono). Cuando se recibe información en un mensaje electrónico, sin importar quien lo haya enviado, se debe ser cuidadoso con los archivos y ligas adjuntas cuando éstas no son esperadas, por ejemplo, un mensaje de un proveedor que pide revisar una cotización no solicitada abriendo un archivo adjunto o dando clic a una liga específica. En tal caso hay que verificar, (por ejemplo, por teléfono) con el remitente del mensaje y/o utilizar herramientas antimalware para verificar el contenido.

En el caso específico del SEECAT el análisis de brecha se realizó mediante las siguientes tablas:

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

Análisis de Brecha (medidas de seguridad existentes VS medidas de seguridad faltantes)				
Código	Pregunta o control	¿Existe?		
		Sí	No	Observaciones
B.	Medidas de seguridad en el entorno de trabajo físico			
B.1.	¿tienes medidas de seguridad para acceder al entorno de trabajo físico?		X	
B.1.1.	Alerta del entorno de trabajo	X		

B.1.2.	Mantener registros del personal con acceso al entorno de trabajo		X	
B.2.	¿Tienes medidas de seguridad para evitar el robo?	X		
B.2.1.	Cerraduras y candados	X		
B.2.2.	Elementos disuasorios		X	
B.2.3.	Minimizar el riesgo oportunista	X		
B.3.	¿Cuidas el movimiento de información en entornos de trabajo físico?		X	
B.3.1.	Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico		X	
B.3.2.	Mantener en movimiento solo copias de la información, no el elemento original	X		
B.3.3.	Usar solo mensajería certificada	X		

Análisis de Brecha (medidas de seguridad existentes VS medidas de seguridad faltantes)				
Código	Pregunta o control	¿Existe?		
		Sí	No	Observaciones
C.	Medidas de seguridad en el entorno de trabajo digital			
C.1.	¿Realizas actualizaciones al equipo de cómputo?	X		
C.2.	¿Revisas periódicamente el software instalado en el equipo de cómputo?		X	
C.3.	¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?	X		
C.3.1.	Uso de contraseñas y/o cifrado	X		
C.3.2.	Uso de contraseñas sólidas	X		
C.3.3.	Bloqueo y cierre de sesiones	X		
C.3.4.	Administrar usuarios y accesos	X		
C.4.	¿Revisas la configuración de seguridad del equipo de cómputo?		X	
C.5.	¿Tienes medidas de seguridad para navegar en entornos digitales?		X	
C.5.1.	Instalar herramientas antimalware y de filtrado de tráfico	X		
C.5.2.	Reglas de navegación segura		X	
C.5.3.	Reglas para la divulgación de información		X	
C.5.4.	Uso de conexiones seguras	X		
C.6.	¿Cuidas el movimiento de información en entornos de trabajo digitales?	X		
C.6.1.	Validación del destinatario de una comunicación	X		
C.6.2.	Seguridad de la información enviada y recibida	X		

ANEXO 4. Programa de Capacitación

I.- Programa de Capacitación en Protección de Datos Personales

Objetivo:

El objetivo principal de este programa es **sensibilizar y capacitar al personal** sobre la importancia de la protección de datos personales en el entorno laboral. Se busca que los servidores públicos comprendan su rol en la salvaguardia de la información personal y adquieran conocimientos básicos sobre el marco legal y teórico relacionado con la privacidad de datos.

Duración:

Este programa consta de **tres sesiones**, cada una de aproximadamente **2 horas**.

Contenido:

1. **Introducción a la Protección de Datos Personales:**
 - Definición y conceptos clave.
 - Importancia de la privacidad en el contexto laboral.
 - Marco legal y normativo (Ley de Protección de Datos Personales, regulaciones específicas, etc.).
2. **Roles y Responsabilidades:**
 - Funciones del servidor público como custodio de datos personales.
 - Responsabilidades del titular de la Unidad Administrativa.
 - Identificación de áreas de riesgo y vulnerabilidad.
3. **Hábitos Seguros y Buenas Prácticas:**
 - Identificación de prácticas que ponen en riesgo la privacidad.
 - Uso adecuado de dispositivos electrónicos y sistemas informáticos.
 - Casos de estudio y ejemplos prácticos.

Metodología:

- Sesiones interactivas con presentaciones, ejemplos y dinámicas.
- Participación activa de los asistentes.
- Evaluación al final de cada sesión.

Recursos:

- **Material de Apoyo:** Se proporcionará una guía impresa con los conceptos clave y referencias legales.
- **Ejemplos y Casos Prácticos:** Se utilizarán ejemplos reales para ilustrar los riesgos y buenas prácticas.

Evaluación:

- **Cuestionario de Conocimientos:** Al finalizar el programa, se aplicará un breve cuestionario para evaluar la comprensión de los participantes.

Resultados Esperados:

- Mayor conciencia sobre la importancia de la protección de datos personales.
- Identificación de hábitos que deben modificarse para garantizar la privacidad.
- Compromiso de aplicar los conocimientos adquiridos en el entorno laboral.

II.- Programa de Capacitación en Tratamiento y Seguridad de Datos Personales

Objetivo:

El objetivo de este programa es **capacitar al personal** de manera específica en relación con sus funciones y responsabilidades en la protección de datos personales. Se busca que las servidoras públicas y los servidores públicos adquieran conocimientos prácticos para atender solicitudes de derechos ARCO, actualizar avisos de privacidad e inventarios de tratamiento, y revisar y mejorar las medidas de seguridad.

Duración:

Este programa se desarrollará a lo largo de **seis meses**, con **una sesión mensual** de aproximadamente **4 horas** cada una.

Contenido:

1. Derechos ARCO y Procedimientos de Atención:

- Identificación de solicitudes de acceso, rectificación, cancelación y oposición.
- Pasos para atender solicitudes de derechos ARCO.
- Documentación y seguimiento.

2. Actualización de Avisos de Privacidad e Inventarios de Tratamiento:

- Revisión y modificación de los avisos de privacidad.
- Identificación de los tratamientos de datos personales.
- Mantenimiento de inventarios actualizados.

3. Medidas de Seguridad y Reducción de Riesgos:

- Evaluación de riesgos y vulnerabilidades.
- Implementación de medidas técnicas y organizativas.
- Actualización periódica de las medidas de seguridad.

4. Casos Prácticos y Talleres:

- Análisis de situaciones reales.
- Simulación de respuestas a solicitudes ARCO.
- Ejercicios de revisión de avisos de privacidad.

Metodología:

- Sesiones presenciales o virtuales.
- Presentaciones, ejemplos y dinámicas.
- Participación activa de los asistentes.
- Evaluación al final de cada sesión.

Recursos:

- **Material de Apoyo:** Guías, formatos y ejemplos.
- **Casos Prácticos:** Estudio de casos reales.

Evaluación:

- **Participación y Evaluación de Conocimientos:** Se evaluará la comprensión y aplicación de los conceptos.

Resultados Esperados:

- Personal capacitado en procedimientos ARCO y seguridad de datos.
- Actualización efectiva de avisos de privacidad e inventarios.
- Reducción de riesgos de vulneración de datos personales.

III.- Programa de Cultura de Seguridad en Tratamiento de Datos Personales

Objetivo:

El propósito principal de este programa es **fomentar una cultura sólida de seguridad de datos personales** en toda la organización. Se busca que todos los miembros del equipo comprendan la importancia de proteger la información personal y se involucren activamente en su salvaguardia.

Duración:

Este programa es continuo y se implementará a lo largo de **varios años** para lograr un cambio cultural sostenible.

Contenido:

1. **Sensibilización y Compromiso:**
 - Comunicación constante sobre la relevancia de la seguridad de datos.
 - Involucramiento de líderes y alta dirección.
 - Creación de un sentido de responsabilidad compartida.
2. **Educación y Formación:**
 - Sesiones de capacitación periódicas para todo el personal.
 - Talleres específicos para áreas clave (TI, recursos humanos, etc.).
 - Actualización constante sobre regulaciones y mejores prácticas.
3. **Integración en Procesos y Políticas:**
 - Revisión y actualización de políticas internas relacionadas con datos personales.
 - Incorporación de medidas de seguridad en los procesos operativos.
 - Evaluación regular de riesgos y vulnerabilidades.
4. **Campañas de Concientización:**
 - Eventos, charlas y actividades para mantener la atención en la seguridad de datos.
 - Reconocimiento de buenas prácticas y logros.

Metodología:

- **Comunicación Continua:** Boletines, correos electrónicos, reuniones.
- **Formación Práctica:** Talleres, ejercicios de simulación.
- **Evaluación de Impacto:** Medición del cambio cultural.

Recursos:

- **Equipo de Capacitación:** Designación de responsables para liderar la formación.
- **Material Didáctico:** Guías, manuales, infografías.

Resultados Esperados:

- **Conciencia Generalizada:** Todos los colaboradores comprenden su papel en la seguridad de datos.
- **Comportamiento Proactivo:** Se adoptan prácticas seguras de manera natural.
- **Cumplimiento Normativo:** La cultura de seguridad se refleja en la operación diaria.

