Oficio No.: **UT/SEDECYT/060/2024**
Asunto: Respuesta a solicitud de transparencia
Aguascalientes, Ags. a 09 de octubre de 2024

**JAVIER MORALES N**
**P R E S E N T E.-**

Por medio de la presente, y en atención a la solicitud de acceso a la información pública con número de identificación **0100516240000047** recibida ante esta **UNIDAD DE TRANSPARENCIA**, le hago entrega de lo solicitado a través de la presente, respondiendo todas y cada una de las preguntas del archivo adjunto a su solicitud, siendo lo siguiente:

1. **¿Qué políticas en materia de protección de datos personales han diseñado y/o implementado?**

   Las que de conformidad a la Ley General de Transparencia y Acceso a la Información Pública se establecen, así como sus relativos y aplicables; por ejemplo, nuestro Aviso de Privacidad integral y simplificado, el cual, se encuentran en **www.aguascalientes.gob.mx/SEDECYT/scii2022,** así como el Documento de Seguridad.

2. Se me entregue el documento de seguridad.

   Se anexa al presente.

3. **¿Qué medidas de seguridad han adoptado para mantener exactos, completos, correcto y actualizados los datos personales?**

   Cada Unidad Administrativa de esta Secretaría, en posesión de datos personales cuenta con sus propias medidas de seguridad, entre ellas, la captura y resguardo de información en archivos digitales y expedientes físicos, con la finalidad de regular su debido tratamiento.

4. **¿Qué procedimientos han establecidos para la conservación y en su caso, bloqueo y supresión de los datos personales?**

   Se ha establecido la identificación de información por cada Unidad Administrativa de esta Secretaría, para su conservación, y en su caso, bloqueo y supresión de los datos personales.

5. **¿Qué procedimientos han implementado y/o desarrollado para recibir y responder dudas y quejas de los titulares de los datos personales y en que consiste?**

   Para recibir, responder dudas y quejas de los titulares de los datos personales se realiza directamente ante esta Unidad de Transparencia de la SEDECYT, o bien por medio del correo electrónico **humberto.ramirez@aguascalientes.gob.mx,** de conformidad con lo establecido en el artículo 58 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Aguascalientes y sus Municipios; en cualquier momento el titular o sus representantes podrá ejercer sus derechos de acceso, rectificación, cancelación u oposición al tratamiento de los datos personales (Derechos ARCO) ante esta Unidad de Transparencia de la SEDECYT, respecto del tratamiento de los datos personales

que le conciernen excepcionalmente en aquellos supuestos previstos por obligación legal, o en su caso, por mandato judicial.

6. **¿Qué mecanismos han utilizados y/o aplicados para cumplir con los plazos fijados para la supresión de los datos personales?**

   Se ha aplicado la identificación de información por cada Unidad Administrativa de esta Secretaría para cumplir con los plazos fijados para la supresión de los datos personales.

7. **En los años 2010 a la fecha, ¿qué mecanismos y/o desarrollado han aplicado para la revisión periódica sobre la necesidad de conservar los datos personales y cuáles son?**

   Se ha aplicado la identificación de información por cada Unidad Administrativa de esta Secretaría para la revisión periódica sobre la necesidad de conservar los datos personales, los cuales, son los Avisos de Privacidad que se van actualizando.

8. **¿Qué códigos de buenas prácticas y/o modelo en materia de protección de datos personales han implementado y/o realizado y/o elaborado, ect.?**

   Se han implementado los Avisos de Privacidad, integral y simplificado, así como elaborado el Documento de Seguridad de la SEDECYT.

9. **¿Qué programas y/o políticas de protección de datos personales han implementado y/o realizado y/o elaborado, ect.?**

   Se han implementado los Avisos de Privacidad, integral y simplificado, así como elaborado el Documento de Seguridad de la SEDECYT.

10. **Solicito su programa de capacitación en materia de datos personales, ¿han aplicado en su institución y/o dependencia de los años 2023 y 2024?**

    Se proporciona el Programa de Capacitación a través del siguiente link: **https://drive.google.com/file/d/1UOnopJBB4e84YfDjxqRky7gmmyHdRJLK/view?usp=sharing**

11. ¿Qué programas y/o políticas de seguridad de datos personales han implementado en su institución y/o dependencia de los años 2023 y 2024 y cuáles son?

    Se han implementado los Avisos de Privacidad, integral y simplificado, así como elaborado el Documento de Seguridad de la SEDECYT 2023 y 2024.

12. **¿Qué programas y/o servicios y/o sistemas y/o plataformas informáticas han realizado y/o implementado y/o diseñado para el tratamiento de los datos personales?**

    La Plataforma Nacional de Transparencia

13. **¿Qué medidas de seguridad han implementado para mantener la seguridad para la protección de los datos personales que permitan protegerlo contra**

14. **daño, y/o pérdida y/o alteración y/o destrucción para garantizar su confidencialidad, integridad y disponibilidad?**

    Se protege la información por parte de cada Unidad Administrativa de la SEDECYT que obtenga datos personales y los mismos son responsables del resguardo, protección y aseguramiento de la información.

15. **Se me entregue en copia escaneada de la bitácora de las vulneraciones de seguridad que han tenido sobre los tratamientos de los datos personales.**

    No se ha presentado el supuesto.

16. **¿Cuántos casos de vulneración han reportado al órgano garante sobre la vulneraciones de los datos personales en los años de 2010 a la fecha?**

    Durante dicho periodo no se ha presentado el supuesto.

17. **¿Qué mecanismos y/o controles han implementado y/o realizado sobre aquellas personas y/o servidores públicos que intervengan para garantizar y guardar la confidencialidad sobre los datos personales que utilizan en sus tratamientos de los datos personales?**

    Control con el Documento de Seguridad a las Unidades Administrativas correspondientes, así como la elaboración y seguimiento de los Avisos de Privacidad, integral y simplificado por parte de las mismas.

18. **¿Cuántas personas y/o servidores públicos manejan datos personales? Se me informen por su nombre de los servidores públicos, área de adscripción y el cargo.**

    Debido a las funciones y atribuciones de esta Secretaría de Desarrollo Económico, Ciencia y Tecnología, el listado de los servidores públicos que manejan datos personales, los encontrará en:
    https://docs.google.com/spreadsheets/d/1wWFGLZOOpw2wVcZbEValJzcWy2LuTbzZ/edit?usp=sharing&ouid=115867833064948730 95&rtpof=true&sd=true

19. **¿Cuántas solicitudes de derechos ARCOP han recibido desde de los años 2010 a la fecha, además se informe por mes cuántas han recibido y esas cuantas ha sido de acceso, rectificación, cancelación, oposición y de portabilidad, y cuántas son hombres y mujeres y cuales se han declarado la inexistencia de los datos personales?**

    Durante dicho periodo no se ha presentado el supuesto.

20. **Copia escaneada del nombramiento de su oficial de protección de datos personales.**

    Se proporciona la designación del oficial de Datos Personales de la SEDECYT, a través del siguiente link:
    https://drive.google.com/file/d/1cZ4LxoYreUXd7vhKBLAkuJh6nRhkltfr/view?usp=sharing

**21. Solicito el programa de capacitación del comité de transparencia y/o unidad de transparencia y/o oficial de protección de datos personales en materia de protección de datos personales de los años 2023 y 2024.**

Se proporciona el Programa de Capacitación a través del siguiente link: https://drive.google.com/file/d/1UOnopJBB4e84YfDjxqRKy7gmmyHdRJLK/view?usp=sharing

**22. Se me informe sobre los procedimientos que han implementado y/o realizado para la eficiencia de la gestión de las solicitudes de derechos ARCOP y que área lo realizó.**

Los procedimientos implementados para la eficiencia de la gestión de las solicitudes de derechos ARCO, se llevan a cabo a través de la Plataforma Nacional de Transparencia, y el ente que lo realiza es el Instituto Nacional de Transparencia

**23. ¿Cuántas transferencias han realizado en materia de datos personales en este año 2024 y que áreas administrativas lo han realizado?**

Durante dicho periodo no se ha presentado el supuesto.

**24. ¿Cuentan con el Programa Integral de Gestión de Datos? en caso de contar con dicho programa se me proporcione.**

Esta Secretría no cuenta con dicho programa, la denominación que corresponde a la SEDECYT el el Documento de Seguridad, anexo al presente.

**25. ¿Qué mecanismos han implementado y/o realizado para asegurar que los datos personales se entregue solo a sus titulares y/o representantes?**

De conformidad al artículo 58 de la Ley de Protección de Datos Personales de Posesión de los Sujetos Obligados del Estado de Aguascalientes y sus Municipios, en cualquier momento, el titular o su representante podrá ejercer sus derechos de acceso, rectificación, cancelación u oposiciñon al tratamiento de sus datos personales (Derechos ARCO), ante la Unidad de Transparencia de la SEDECYT, respecto del tratamiento de los datos personales que le conciernen excepcionalmente en aquellos supuestos previstos por obligación legal, o en su caso, por mandato judicial.

Para el ejercicio de los Derechos ARCO, será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante. El titular podrá acreditar su identidad mediante identificación oficial, instrumentos electrónicos o mecanismos de autentificación fehaciente, o mediante aquellos mecanismos establecidos de manera previa, siempre y cuando permitan de forma inequívoca la acreditación de la identidad del titular.

**26. ¿Cuantos servidores públicos integran su unidad de transparencia?**

Un servidor únicamente.

**27. ¿Cuántas auditorías en materia de datos personales le han solicitado al órgano garante desde el 2010 a la fecha?**

Durante dicho periodo no se ha presentado el supuesto.

**28. Se me informe si han remitido el informe semestral referente al número de requerimientos de localización geográfica en tiempo real y de registro de datos realizados, así como el número de registros de datos de comunicaciones cancelados y suprimidos de manera segura, una vez cumplido el fin para el cual fueron solicitados, de los años 2010 a la fecha.**

No se ha remitido informe semestral alguno, puesto que no se encuentra prevista la obligación de entregar informe semestral referente al número de requerimientos de localización geográfica en tiempo real y de registro de datos realizados; y no se ha presentado el supuesto de registro de datos de comunicaciones canceladas y/o suprimidos de manera segura.

**29. Referente al informe antes solicitado se me entregue el link donde pueda consultar la información estadística de dicho informe.**

Debido a la respuesta de la pregunta anterior, no existe dicho informe.

**30. ¿Cuántas denuncias en materia de datos personales han recibido desde el años 2010 a la fecha?**

Durante dicho periodo no se ha presentado el supuesto.

**31. Se me explique cuáles son las medidas que aplican para uno de los principios incorporados en la LGPDPPSO, para garantizar el tratamiento de los datos personales.**

Entre las medidas que se aplican, se encuentra la que los responsables del tratamiento de datos personales deben sujetarse a las facultades y atribuciones que la normatividad aplicable les confiere, en ese sentido, se sujetan a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

**32. ¿Qué sujetos obligados han presentado su evaluación de impacto en la protección de datos personales en los años 2020 a la fecha?**

Durante dicho periodo no se ha presentado el supuesto.

**33. ¿Cuántas recomendaciones no vinculantes han emitido sobre el contenido de la evaluación de impacto de los años 2020 a la fecha?**

Durante dicho periodo no se ha presentado el supuesto.

**34. ¿Cuántas denuncias en materia de obligaciones de transparencia han recibido desde el año 2020 a la fecha y el sentido de la resolución?**

Durante dicho periodo no se ha presentado el supuesto.

**35. ¿Qué programa y/o acciones han implementado en materia de gobierno abierto?**

A través de la página web del Gobierno del Estado de Aguascalientes, en la sección de la Secretaría de Desarrollo Económico, Ciencia y Tecnología, en la pestaña de

Transparencia, se encuentra el apartado de Gobierno Abierto, en el cual se puede consultar información de interés y utilidad a la ciudadanía.

Agradeciendo de antemano su atención, y quedando a la orden para cualquier duda o aclaración, le envío un cordial saludo.

Atentamente,

**LIC. LUIS HUMBERTO RAMÍREZ**
**TITULAR DE LA UNIDAD DE TRANSPARENCIA DE LA SECRETARÍA DE DESARROLLO ECONÓMICO, CIENCIA Y TECNOLOGÍA DEL ESTADO DE AGUASCALIENTES.**

"2024, AÑO DEL BICENTENARIO DE LA CONSTITUCIÓN FEDERAL DE LOS ESTADOS UNIDOS MEXICANOS DE 1824".

**DOCUMENTO DE SEGURIDAD**
**UNIDAD DE TRANSPARENCIA DE LA**
**SECRETARÍA DE DESARROLLO ECONÓMICO, CIENCIA Y TECNOLOGÍA.**

Lic. Luis Humberto Ramírez
Titular de la Unidad de Transparencia
Fecha de elaboración: 04 de enero de 2024.

## DEFINICIONES PARA EL DOCUMENTO DE SEGURIDAD

Para los efectos del presente documento, se tomarán las definiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, sin perjuicio de lo previsto en la normativa aplicable en la materia, se entenderá por:

**Áreas responsables:** Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento y ser responsables o encargadas de los datos personales y que deciden sobre el tratamiento de datos personales.

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

**Bases de datos:** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

**Bloqueo:** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de dichas responsabilidades. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

**Cómputo en la nube:** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales y el uso de recursos compartidos de manera dinámica.

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

**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 políticas y preferencia sexual.

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

**Disociación:** El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

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

**Encargado:** La persona física o 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.

**Medidas compensatorias:** Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance.

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

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

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

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

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

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

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

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

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

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

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

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

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

**Supresión:** La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

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

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

## PRESENTACIÓN

La Unidad de Transparencia de la Secretaría de Desarrollo Económico, Ciencia y Tecnología reconoce que la información que se recaba, genera, procesa y resguarda, debe ser tratada en estricto apego al marco legal aplicable durante todo su ciclo de vida y preservando, en todo momento, el derecho de protección de datos personales de todas las personas, incluyendo servidores públicos, lo cual es responsabilidad de todos aquellos que, en el estricto apego a sus funciones, tratan esta información.

## MARCO NORMATIVO

Artículos 6, Base A y 16 párrafo segundo de la Constitución de los Estados Unidos Mexicanos; Artículo 3, Título Primero. Capítulos I y II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; Títulos Sexto y Séptimo de la Ley General de Transparencia y Acceso a la Información Pública.

## SISTEMA DE GESTIÓN

### 1.- INVENTARIO DE DATOS PERSONALES Y SISTEMAS DE TRATAMIENTO

| INVENTARIO DE DATOS PERSONALES | | | | |
|---|---|---|---|---|
| **Fecha de Recepción de Datos Personales** | **Datos Personales Sometidos a Tratamiento** | **Finalidad del Tratamiento** | **Transferencia de Datos Personales** | **Periodo de Conservación de Datos Personales** |
| (Día/mes/año) | (Especificar sólo el tipo de dato personal recabado: RFC, correo, INE, domicilio, teléfono particular, cuenta bancaria, comprobante de estudios, etc.) | (obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, etc.) | (Señalar de forma específica a quien se le realiza la transferencia de datos personales y/o remisión)<br><br>(Si no hay transferencia y/o remisión de datos personales, poner "NA") | (Señalar Periodo de Conservación necesario para el cumplimiento de las finalidades que justificaron su tratamiento)<br><br>(Asimismo referir, en su caso, si hay bloqueo o supresión de datos personales) |

| Etapa del Ciclo de Vida en la que se Encuentran los Datos Personales | | | |
|---|---|---|---|
| **Obtención** | **Uso** | **Bloqueo** | **Supresión** |
| X | X | X | X |

| SISTEMAS DE TRATAMIENTO<br>Bases de Datos | |
|---|---|
| **Físicos** | **Digitales** |
| (Recepción de Información Documental; Trámite; Servicio; Expedientes; Acuerdos; Resoluciones, etc.) | (Plataforma Nacional de Transparencia; Cómputo en la Nube; Correo Electrónico; CD, Word; Excel; Unidades de Almacenamiento; etc.) |

| Ejercicio de Derechos ARCO | | | | |
|---|---|---|---|---|
| **Acceso** | **Rectificación** | **Cancelación** | **Oposición** | **No aplica** |
| X | X | X | X | X |
| **Consentimiento Expreso del Titular de los Datos Personales** | | | | |
| **Difundir** | **Distribuir** | **Comercializar** | | **No se otorgó consentimiento expreso** |
| X | X | X | | X |

## 2.- FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

| | |
|---|---|
| **Unidad administrativa:** | (Señalar nombre de la unidad administrativa a cargo o administradora del proceso o procedimiento en el que se tratan los datos personales) |
| **Nombre del Responsable o Encargado del Tratamiento de Datos Personales:** | (Nombre completo y señalar si es Responsable o Encargado) |
| **Empleo, Cargo o Comisión del Responsable o Encargado:** | (Especificar) |
| **Atribuciones de la Unidad Administrativa:** | (Señalar las atribuciones específicas de la unidad administrativa, entre ellas, las que señala la Ley Orgánica, Reglamento de Trabajo, etc.) |
| **Fundamento Jurídico que habilita el tratamiento:** | (Señalar las principales disposiciones normativas, artículos, apartados, fracciones, incisos, párrafos de los que deriva el tratamiento en cuestión) |

## 3.- ANÁLISIS DE RIESGOS

| Tipo de Datos Personales | Número de Personas que dan Tratamiento de Datos Personales | Sitios de Resguardo | Nivel de Riesgo Inherente (Bajo, Medio, Alto, Reforzado) |
|---|---|---|---|

| | | | |
|---|---|---|---|
| (Información concerniente a una persona física identificada o identificable) | (Número) | (Oficinas, Escritorio, Cajones, Archiveros, Carpetas, Organizadores, Cajas, Espacio Destinado para el Tratamiento, Computadoras, Laptops, Servidores, Unidades Externas, etc.) | (Bajo: considera información general concerniente a una persona física identificada o identificable)<br><br>(Medio: permiten conocer la ubicación física de la persona, su patrimonio, datos de autenticación o jurídicos)<br><br>(Alto: contempla datos personales sensibles)<br><br>(Reforzado: de acuerdo a su naturaleza pueden derivar en mayor beneficio para un atacante, por ejemplo: información adicional como códigos de seguridad, números de identificaciones personales, o relacionados con niveles de primer mando, figuras públicas, líderes, o información relacionada con la impartición de justicia o seguridad nacional) |

| **AMENAZAS** | | |
|---|---|---|
| **Origen de la Amenaza** | **Motivación/Causa** | **Posibles Consecuencias** |
| (Hacker; Cracker; Criminal Computacional, etc.) | (Desafío; Dinero; Ego; Estatus; Rebelión; Alteración no Autorizada de Información; Destrucción de Información; Ganancia Económica; Revelación Ilegal de Información; etc.) | (Acceso No Autorizado al Sistema; Ingeniería Social; Intrusión en los Sistemas; Robo de Información, Código Malicioso; etc.) |
| (Intencional; Terrorista; Beneficio, etc.) | (Chantaje; Destrucción; Explotación; Ganancia Política; Reconocimiento Mediático; Venganza, etc.) | (Ataque a Personas y/o Instalaciones; Vulneración a la Seguridad; Ataque a Sistemas; Manipulación de los Sistemas; Acceso Indebido a los Sistemas, etc.) |
| (Espionaje) | (Espionaje Económico; Ventaja Competitiva; Ganancia Política, etc.) | (Acceso No Autorizado a Información Clasificada como Reservada o Confidencial; Explotación Económica; Intrusión a la Privacidad del Personal o a los Sistemas; Robo de Información; Ventaja Política; etc.) |
| (Interno. - Personal No Capacitado; Descontento; Negligente; Deshonesto; | (Curiosidad; Ego; Errores No Intencionales u Omisiones; Ganancia Económica; Venganza, etc.) | (Abuso en la Operación de los Sistemas; Acceso No Autorizado a los Sistemas; Ataque a Empleados y/o Instalaciones; Chantaje; |

| | | |
|---|---|---|
| Empleado Despedido, etc.) | | Código Malicioso; Consulta y Uso de Información Clasificada como Reservada o Confidencial; Errores en los Sistemas; Fraude y Robo; Intercepción de Comunicaciones; Intrusiones a Sistemas; Venta de Información; etc.) |

| **VULNERABILIDADES EXISTENTES** | |
|---|---|
| (Personal) | (Falta de Personal Sensibilizado y/o Entrenado en Seguridad; Proceso de Reclutamiento Inadecuado; Uso Incorrecto de Software y Hardware; Falta de Supervisión al Trabajo de Externos; Falta de Políticas Acerca del Uso de Medios de Telecomunicaciones, etc.) |
| (Acciones No Autorizadas) | (Uso No Autorizado de Equipo; Uso de Software Malicioso, etc.) |
| (Daño Físico) | (Fuego; Agua; Contaminación; Accidentes; Polvo; Corrosión; Humedad; Congelamiento, etc.) |
| (Eventos Naturales) | (Fenómenos Climáticos o Meteorológicos; Fenómenos Sísmicos; Fenómenos Volcánicos, etc.) |
| (Pérdida de Servicios Básicos) | (Falla en el Sistema de Aire Acondicionado o Suministro de Agua; Pérdida de Suministro Eléctrico; Falla en los Equipos de Telecomunicaciones, etc.) |
| (Información Comprometida por Fallas Técnicas) | (Intercepción e Interferencia de Señales; Espionaje Remoto; Escucha en Comunicaciones; Robo de Medios o Documentos; Robo de Equipo; Recuperación de Medios Desechados o Reciclados; Revelación; Fuentes Poco Confiables para la Obtención de Datos; Alteración de Hardware; Alteración de Software; Rastreo de Localización; Fallas del Equipo; Malfuncionamiento del Equipo; Saturación de los Sistemas de Información; Malfuncionamiento del Software; Falla en el Mantenimiento del Sistema de Información, etc.) |
| (Incumplimiento de Funciones) | (Error de Uso; Abuso de Privilegios; Falsificación de Privilegios; Denegación de Acciones, etc.) |
| (Hardware) | (Mantenimiento Insuficiente; Equipos No Actualizados; Falta de Configuraciones Adecuadas al Equipo; Susceptibilidad a las Variaciones del Ambiente; Cambios de Voltaje; Almacenamiento No Cifrado; Falta de Cuidado en la Destrucción de Soportes Electrónicos; etc.) |
| (Software) | (Carencia o Falta de Pruebas al Software y su Configuración; Falta de Actualizaciones; No Cerrar la Sesión; Desecho o Reutilización de Medios de Almacenamiento sin un Adecuado Borrado de Información; Falta de Registros de Auditoría; Error en las Asignaciones de Privilegios de Acceso; Interfaces de Usuario Complicadas; etc.) |
| (Redes) | (Falta de Mecanismos de Identificación y Autenticación de Usuario; Contraseñas No Cifradas; Servicios de Red Innecesarios; Mal Uso de Protocolos; Falta de Monitoreo de los Componentes de las Redes, Servicios y Aplicaciones; Descarga y Uso de Software No Controlado; Falta de Respaldos; Falta de un Registro sobre la Administración de los Recursos; Líneas de Comunicación Sin Protección; Cableado de Interconexión Dañado o Antiguo; Arquitectura de Red Insegura, etc.) |
| (Sitio) | (Falta o Implementación Inadecuada de Controles de Acceso; Lugar Susceptible al Daño por Agua; Red Eléctrica Inestable, etc.) |
| (Organización) | (Falta de Procedimientos Formales para la Administración de Privilegios de Usuario; Falta o Insuficiencia de Previsiones en la Realización de Contratos con Terceros; Falta de Procedimientos Formales de Monitoreo |

| | |
|---|---|
| | y/o Auditoría; Falta o Ausencia de Reportes de Fallas; Falta de Procedimiento Formal para Supervisar y Documentar; Falta de Asignación de Responsables Respecto a la Seguridad de la Información; Falta de Políticas de Uso de Correo Electrónico; Falta de Procedimientos para la Instalación y Actualización de los Sistemas de Información; Falta de Registros de Actividades o Bitácoras en los Sistemas de Administración u Operación; Falta de Procesos para el Tratamiento de Datos Personales; Falta o Insuficiencias de Condiciones Relacionadas a la Protección de Datos en Contratos con Empleados; Falta de Procesos Estrictos en Caso de un Incidente o Vulneración de Seguridad; Falta de Políticas para el Uso de Información Fuera de la Organización; Falta de Mecanismos de Monitoreo para Vulneraciones a la Seguridad de los Datos; Falta de Procedimientos para Reportar Puntos Débiles en la Seguridad, etc.) |

| **Recursos Involucrados en el Tratamiento de Datos Personales** | | | | | | |
|---|---|---|---|---|---|---|
| **Físico** | **Internet** | **Wifi** | **Red Interna** | **Red de Terceros** | **Hardware** | **Software** |
| X | X | X | X | X | X | X |

## 4.- ANÁLISIS DE BRECHA

| Medidas de Seguridad Existentes | Medidas de Seguridad Faltantes |
|---|---|
| (Físicas/Técnicas – Descripción; Asimismo, revisar los Controles y Parámetros contenidos en el siguiente numeral, que en su caso apliquen, y señalarlos en este apartado) | (Físicas/Técnicas - Descripción; Asimismo, revisar los Controles y Parámetros contenidos en el siguiente numeral, que en su caso apliquen, y señalarlos en este apartado) |

## 5.- PLAN DE TRABAJO

Se elaborará 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; entre las cuales se pueden encontrar las siguientes:

| **Control** | **Parámetro** |
|---|---|
| **Políticas** | |
| (Políticas de Gestión de Datos Personales) | Deben existir políticas aprobadas para la regulación específica, condiciones contractuales, así como para la creación, implementación y mantenimiento de los diferentes controles establecidos para salvaguardar los datos personales y sus activos relacionados durante el tratamiento, que sirvan como guía organizacional del propósito, objetivos, responsabilidades y compromisos establecidos por los involucrados para el cumplimiento de la normatividad aplicable a los datos personales. |
| (Revisión y Evaluación) | Las políticas implementadas deben ser revisadas y evaluadas en su efectividad y cumplimiento periódicamente, así como cuando surja un nuevo riesgo o cambio significativo en la organización. |
| (Identificación y Documentación) | Se debe identificar y documentar de manera proporcional a la organización la información, políticas, acuerdos, planes estratégicos, procedimientos, controles de seguridad, y todo proceso relacionado. |
| **Cumplimiento Legal** | |

| | |
|---|---|
| (Identificación de Legislación/Regulación Aplicable) | Se deben identificar y documentar los deberes y responsabilidades de toda la organización para cumplir con los requerimientos legales y contractuales relacionados con la protección de datos personales. Se debe poner especial atención en la legislación relacionada con la propiedad intelectual, industrial, privacidad y protección de datos personales a nivel nacional e internacional. También se debe considerar la regulación específica de un sector o rama industrial. |
| (Salvaguarda de Registros Organizacionales) | Se debe mantener el resguardo de todos los registros y documentación que pudieran ser evidencia o bien, protegerlos contra pérdida, destrucción, falsificación, acceso o revelación no autorizados. |
| (Prevención del Mal Uso de la Información) | Se deben tener mecanismos contra el uso de información para propósitos no autorizados, por ejemplo, para sistemas electrónicos, utilizar bloqueos en caso de que usuarios no autorizados traten de acceder a módulos que no tienen permisos e informar mediante un mensaje el uso indebido. |
| (Recolección de Evidencia) | Se deben tener procesos para la recolección de evidencia según las mejores prácticas en caso de una vulneración o incidente de seguridad. |
| (Revisión de Cumplimiento Técnico) | Se deben revisar los activos y sus controles de seguridad, tal que se verifique su correcto funcionamiento, así como las posibles amenazas y vulnerabilidades relacionadas. |
| (Controles de Auditoría de Sistemas) | Se debe tener un proceso para la revisión y evaluación del funcionamiento de los sistemas, tal que se minimicen las consecuencias de posibles vulneraciones y se logre un ciclo de mejora continua. |
| (Protección del Soporte de Auditoría del Sistema) | Se deben proteger las herramientas, el software y los archivos de datos que surjan o se utilicen en una auditoría, para evitar comprometer la seguridad de la información de la organización. |
| | **Estructura Organizacional de la Seguridad** |
| (Administración y Coordinación de la Seguridad de la Información) | Debe tener claros sus objetivos y soportar las iniciativas generadas por su equipo, apoyados en la comunicación efectiva entre las diferentes áreas de la organización para la implementación de controles de seguridad, coordinados por la persona a cargo de la seguridad de la información personal. |
| (Designación de Deberes en Seguridad y Protección de Datos Personales) | Se deben designar deberes y obligaciones respecto a los individuos que intervengan en el uso y protección de datos personales. |
| (Recomendaciones de un Especialista en Seguridad de la Información) | Cuando sea adecuado, obtener el consejo y recomendaciones de un especialista en protección de datos y seguridad de la información. |
| (Cooperación con Organizaciones) | En su caso, buscar la colaboración de autoridades, cuerpos regulatorios, servicios de información o de telecomunicaciones, entre otros para definir las acciones apropiadas en caso de un incidente o vulneración de seguridad. |
| (Identificación de Riesgos de Terceros) | Identificar el alcance de involucramiento que pueden tener terceros en el tratamiento de los datos personales y analizar si es justificado y bajo el consentimiento del titular. |
| (Requerimientos de Seguridad en Contratos con Terceros) | Cuando se establezca un contrato con un tercero, revisar las cláusulas referentes a los requerimientos de seguridad y de tratamiento de datos personales para verificar su correspondencia con los requerimientos de la organización. Se debe revisar el contrato generado entre la organización y el prestador respecto al nivel de servicio, incluyendo cualquier actualización de los términos y condiciones. Esto es |

| | |
|---|---|
| | importante en el caso de la designación de encargados por parte de un responsable de datos personales. |
| (Requerimientos de Seguridad en Contratos con Servicios de Almacenamiento de Información y Computo en la Nube) | Cuando se establezca un contrato con un prestador de servicios de almacenamiento de información y/o de cómputo en la nube, además de revisar las cláusulas referentes a los requerimientos de seguridad y de tratamiento de datos personales, de manera particular hay que: verificar el nivel de acceso que tiene el prestador y limitar el tratamiento a lo estrictamente necesario para el cumplimiento de las condiciones del servicio; verificar el ciclo de vida de la información (por ejemplo, dónde se almacena, cómo se replica, cómo se elimina en un ambiente distribuido, como se garantiza la eliminación de la información) y la ubicación física de la infraestructura del prestador. |
| **Clasificación y Acceso a la Información** | |
| (Inventario y Clasificación de Datos Personales) | Mantener un registro de los datos personales recolectados y tratados por la organización en cualquier soporte físico o electrónico, teniendo especial atención en los datos sensibles, financieros y patrimoniales. |
| (Identificación de Procesos de Datos Personales) | Se debe tener identificado el ciclo de vida de los datos personales en cada uno de sus procesos, desde la obtención, almacenamiento, procesamiento, cancelación o cualquiera que sea su tratamiento. Esto es especialmente importante para conocer dónde se resguardan y qué se hace con los datos personales, lo cual contribuye también en agilizar la respuesta al ejercicio de los derechos ARCO por parte de un titular. |
| **Seguridad del Personal** | |
| (Identificar Responsabilidades de Seguridad en cada Puesto de Trabajo) | Establecer y dar a conocer a cada, función, rol o puesto las responsabilidades que corresponden respecto a la seguridad y protección de datos personales, informando en su caso de las sanciones de incumplimiento de la política de seguridad. |
| (Revisión de Contratación del Personal) | Revisar el perfil del personal que será contratado por la organización, esto debe incluir referencias (personales y/o laborales), la confirmación de títulos académicos y profesionales, así como los controles de identidad y antecedentes. |
| (Acuerdo de Confidencialidad) | Se debe firmar un acuerdo de confidencialidad o no revelación de información por los nuevos empleados de la organización involucrados en el tratamiento de los datos personales. |
| (Términos y Condiciones de Empleo) | Dentro de los términos de contratación, la organización debe informar ampliamente a los nuevos empleados sobre sus deberes y compromisos respecto a la seguridad de la información y protección de datos personales. También deberá considerarse la presentación de un aviso de privacidad al personal interno del cual recabaremos datos personales de distintos tipos. |
| (Capacitación) | Empleados, contrataciones externas y usuarios en general deben recibir concienciación y capacitación apropiado respecto a la seguridad de la información y protección de datos personales. |
| (Proceso Disciplinario) | Debe existir un proceso disciplinario en la organización para aquellos que no cumplan o violenten lo establecido en la política o procedimientos. |
| **Seguridad Física y Ambiental** | |
| (Perímetro de Seguridad) | Identificar o en su caso, implementar mecanismos de seguridad en el perímetro de la organización, por ejemplo, bardas, puertas con control de acceso, vigilancia por guardias de seguridad, etc. |
| (Control de Entrada y Salida Física) | Implementar mecanismos que sólo permitan el acceso y salida a personal autorizado, por ejemplo, a través de dispositivos biométricos, tarjetas inteligentes, personal de seguridad, etc. |

| | |
|---|---|
| (Seguridad en Entornos de Trabajo) | Implementar mecanismos para mantener las áreas de resguardo o servicios de procesamiento de datos, aisladas de amenazas causadas por el hombre. Por ejemplo, puertas con cerradura, gabinetes o cajas de seguridad. Además, deben existir mecanismos para proteger la información de fenómenos como el agua, fuego, químicos, vibraciones, radiación, etc. Por ejemplo, extintores, detectores de humo, etc. así como cierto monitoreo ambiental y de medidas comunes, como no introducir alimentos y bebidas en áreas restringidas. |
| (Trabajo en Áreas Restringidas) | Los activos de información sólo deben ser accesibles por personal que los requiera en sus deberes en la organización o bien por un tercero autorizado. Por lo tanto, debe existir acceso controlado para personal trabajando en un área restringida. |
| (Seguridad del Cableado) | Verificar el buen estado de las conexiones de telecomunicaciones o de transmisión de información, para evitar intercepción o falla en el servicio. |
| (Mantenimiento del Equipo) | Asegurarse de que los activos secundarios reciban mantenimiento periódicamente (por ejemplo, según indicaciones del fabricante), además de realizarse por personal autorizado. |
| (Aseguramiento de Información fuera de las Instalaciones) | Se deben establecer mecanismos autorizados, para controlar la salida fuera de las instalaciones de cualquier información que contenga datos personales, considerando que su seguridad sea equivalente al menos a la establecida dentro de la organización. |
| (Borrado Seguro de Información) | Cuando se elimine un activo como equipo de procesamiento, soporte físico o electrónico, deben aplicarse mecanismos de borrado seguro o, bien, de destrucción adecuada. Cualquier eliminación de activos debe registrarse con fines de auditoría. |
| (Escritorio Limpio) | Cualquier documento o activo de información crítico debe estar resguardado, fuera de la vista, cuando éste no sea atendido. |
| (Robo de Propiedad) | Revisar e identificar los activos, como equipo o software que sean susceptibles de sustracción de las instalaciones. |
| **Gestiones de Comunicaciones y Operaciones** | |
| (Control de Cambios Operacionales) | Debe existir un procedimiento para discutir, documentar y evaluar cualquier cambio que pueda afectar las operaciones relacionadas con datos personales. |
| (Segregación de Tareas) | En relación con la estructura de la organización se deben segregar y aislar los puestos y responsabilidades del personal que realice tratamiento de datos personales, con el fin de reducir las oportunidades de un uso indebido de la información. |
| (Separación del Área de Desarrollo de Sistemas de Datos Personales) | Las instalaciones de desarrollo y/o pruebas deben estar aisladas de las áreas operacionales. Por ejemplo, el software de desarrollo debe estar en una computadora diferente al software de producción. La separación puede hacerse a varios niveles, como utilizar distintos segmentos de red, dividir las instalaciones físicas o separar los activos. |
| (Administración Externa de Instalaciones) | Se deben identificar los riesgos derivados del servicio de administración de instalaciones prestado por un proveedor (por ejemplo, instalaciones eléctricas o telefonía). En caso de que se identifique algún riesgo, debe ser discutido con el externo para incorporar los controles adecuados. |
| (Estándares de Configuración Segura y Actualización de Sistemas) | Se deben tener identificadas las necesidades de nuevos sistemas, actualizaciones o nuevas versiones. Es recomendable realizar pruebas antes de implementar cualquiera de ellos. También deberá verificarse que los sistemas que soportan el tratamiento de datos personales cuentan con configuraciones seguras en el hardware, sistema operativo, base de datos y aplicaciones. |

| | |
|---|---|
| (Protección Contra Software Malicioso) | Deben existir diferentes controles respecto al software malicioso: Prohibir el uso de software ilegal y/o no autorizado. Aplicar difusión (campañas, boletines) sencillos para advertir del software malicioso. Mantener en los dispositivos de procesamiento de información como computadoras, las respectivas herramientas actualizadas que las protejan contra software malicioso. En su caso, monitorear el tráfico y las actividades de red para descubrir cualquier comportamiento anómalo, tales como virus, descargas de contenido inapropiado, fugas de información, etc. |
| (Respaldo de la Información) | Deben establecerse respaldos proporcionales al modelo de negocio y manejo de datos personales. Se debe tener un adecuado control sobre la periodicidad de generación de respaldos y el respectivo almacenaje de los soportes físicos/electrónicos, especialmente para el ejercicio de derechos ARCO. Se debe tener identificado el proceso a realizar en caso de que sea necesario restaurar un respaldo, asimismo, se deben probar los respaldos periódicamente para asegurar su correcto funcionamiento. |
| (Registros de Operadores) | Los administradores de los sistemas de datos personales deben poder acceder a los registros de las actividades dentro del mismo, para analizarlos periódicamente. |
| (Registro de Fallas) | Las fallas en sistemas y activos deben poder reportarse y gestionarse, esto incluye la corrección de la falla y revisión de los registros. |
| (Controles de Red) | Cuando aplique, debe existir separación entre los segmentos de red y administración de recursos de red. Deben existir procedimientos y responsabilidades para el manejo de conexiones remotas. Se debe buscar la implementación de controles especiales para salvaguardar la confidencialidad e integridad de las comunicaciones sobre redes públicas (por ejemplo, redes privadas virtuales, métodos de cifrado, etc.) |
| (Gestión de Soportes Informáticos Extraíbles) | Deben existir políticas y procedimientos para el uso de soportes informáticos extraíbles como memorias USB, discos, cintas magnéticas, etc. |
| (Documentación de Seguridad del Sistema) | Toda la documentación de los sistemas y activos de información debe ser protegida de acceso no autorizado. |
| (Seguridad de Medios en Tránsito) | Se debe asegurar el traslado de soportes físicos/electrónicos que contengan datos personales contra robo, acceso, uso indebido o corrupción. |
| (Comercio Electrónico Seguro) | Se deben contar con mecanismos contra la actividad fraudulenta, disputas contractuales o revelación/modificación de información. En los entornos web deben existir mecanismos de autorización y autenticación para las transacciones. Asimismo, debe revisarse las cláusulas de intercambio de datos personales y seguridad en los acuerdos establecidos entre las partes involucradas. |
| (Mensajería Electrónica) | Se debe hacer uso adecuado del correo electrónico, mensajería instantánea y redes sociales, utilizando mecanismos que permitan bloquear la recepción de archivos potencialmente inseguros, mensajes no solicitados, no deseados o de remitente no conocido. |
| (Seguridad en Sistemas Electrónicos) | Se debe hacer uso adecuado de los sistemas de datos personales a través de guías de uso y gestión de riesgos asociados con dichos sistemas. |
| (Divulgación de Información de manera Pública) | Debe existir un proceso de autorización formal para hacer pública información, por cualquier medio de difusión. Cuando se publica un discurso o una nota de prensa, o bien para sistemas de acceso público (por ejemplo, páginas web para publicación de concursos, rifas, entre |

| | |
|---|---|
| | otros), deben existir mecanismos para que la información mantenga su integridad y que no permita ser el medio para dañar otros activos ubicados dentro de la organización. |
| (Otras Formas de Intercambio de Información) | Se debe contar con procedimientos relacionados al intercambio de datos personales, dentro y fuera de la organización a través de diversos medios, como voz, datos, video, etc. El personal debe mantener la confidencialidad de información sensible y datos personales en cualquier intercambio de información. |
| (Disociación y Separación) | Se deben aislar los datos de manera que por sí mismos no aporten información valiosa de un titular o éste no pueda ser identificable. También pueden ser separados los activos de información grandes en activos de información más pequeños (por ejemplo, una base de datos de clientes en dos bases de datos, clientes corporativos y personas físicas). Entre mayor cantidad de información tiene un activo, éste resulta más atractivo para un atacante. |
| **Control de Acceso** | |
| (Reglas de Control de Acceso) | Deben existir reglas y privilegios para cada usuario o grupo de usuarios conforme a sus responsabilidades. |
| (Gestión de Usuarios y Contraseñas) | Cada usuario debe tener un identificador único en el sistema al cual se vincularán sus privilegios y acceso. Asimismo, cada usuario deberá ser responsable de guardar en secreto la(s) contraseña(s) y/o mecanismos correspondientes para su acceso (cuando aplique, los usuarios tendrán que firmar acuerdos que los obliguen a mantener sus contraseñas en secreto). Los usuarios deben tener guías o recomendaciones para la creación y mantenimiento de contraseñas seguras. Se deben tener procedimientos para la administración de usuarios (altas, bajas y modificaciones) en los sistemas de información, en su caso, además, deben existir controles respecto a las contraseñas entregadas al personal, clientes, proveedores, prestadores de servicios o cualquier usuario del sistema de datos personales (por ejemplo, rendición de cuentas, fortalecimiento de contraseñas, almacenamiento cifrado de contraseñas, etc.) |
| (Gestión de Privilegios) | En un ambiente multiusuario se deben conceder privilegios en función de los roles y responsabilidades de cada usuario o grupo de usuarios para el cumplimiento de sus deberes, sin que se exponga a acceso, eliminación copia o alteración no autorizados a otros activos de información. |
| (Revisión de Privilegios de Usuarios) | Debe existir un proceso de revisión para verificar el adecuado y no excesivo uso de los privilegios de cada usuario en función de sus roles y responsabilidades, por ejemplo, una persona con privilegios especiales puede ser revisada cada 3 meses, mientras que un usuario estándar cada 6 meses. |
| (Equipos Sin Atender) | Los usuarios y contrataciones externas deben tener conocimiento de las medidas de seguridad necesarias para cualquier dispositivo de procesamiento sin atender, por ejemplo, cerrar la sesión cuando se ha terminado de trabajar en la computadora, bloquear el equipo automáticamente cuando no se usa por largos periodos de tiempo, etc. |
| (Uso de Servicios de Red) | Deben existir reglas respecto al acceso autorizado a las redes y servicios disponibles, así como los procedimientos de uso y conexión. |
| (Ruta Reforzada) | Cuando aplique, deben existir mecanismos para asegurar un camino único de interconexión entre dispositivos. |

| | |
|---|---|
| (Autenticación de Usuario para Conexiones Externas) | Deben existir mecanismos para asegurar las conexiones que se hagan a través de redes externas a la organización, por ejemplo, cifrado, protocolos de autenticación por desafío mutuo, etc. |
| (Autenticación de Nodo) | Si es el caso, aplicar un método de autenticación alternativo para grupos de usuarios remotos que se conecten a una instalación segura u ordenador compartido. |
| (Segregación de Redes) | La red debe segregar a los usuarios a través de mecanismos como VPN o firewalls, por ejemplo, la red externa para usuarios de visita debe encontrarse en un segmento de red distinto de la red donde se encuentran los sistemas de datos personales. |
| (Protocolos de Conexión de Red) | Se deben vigilar los protocolos de conexión de redes compartidas que se extienden más allá de la organización, por ejemplo, para el correo electrónico o para el acceso a internet. |
| (Protocolos de Enrutamiento) | Se debe vigilar la existencia de mecanismos para asegurar que las conexiones de computadoras y flujos de información no vulneren el control de acceso a la organización. |
| (Seguridad de Servicios de Red) | La organización debe obtener una clara estructura y descripción de los servicios de red públicos o privados, sus características y atributos de seguridad. |
| (Identificación Automática de Terminales) | Contar con un mecanismo de red interna para autenticar cualquier tipo de conexión. |
| (Proceso de Inicio de Sesión) | Sólo se debe tener acceso a los sistemas de datos personales a través de un inicio de sesión seguro, esto minimiza los accesos no autorizados. |
| (Alerta de Coerción a Usuarios) | Cuando aplique, considerar alertas para usuarios cuyos privilegios los hagan objetivo de coerción. |
| (Tiempo Límite de Terminal) | Aquellas terminales que estén expuestas en áreas de acceso general deben configurarse para limpiar la pantalla o bloquearse después de un periodo de inactividad. |
| (Tiempo Límite de Conexión) | Debe existir un tiempo límite de acceso al sistema de datos personales, especialmente para conexiones desde terminales o dispositivos fuera del perímetro de la organización. |
| (Restricción de Acceso a Datos Personales) | El acceso a datos personales a través del personal o aplicaciones debe ser definido en consistencia con la política de seguridad de los datos personales, limitando el uso de información a las responsabilidades específicas. |
| (Trazabilidad de Tratamiento) | La trazabilidad y posibilidad de identificar quién tuvo acceso a los datos personales y los tratamientos realizados. |
| (Aislamiento de Sistemas Sensibles) | Se deben evaluar los sistemas y activos que por su naturaleza deban desarrollarse en ambientes aislados, por ejemplo, equipos ejecutando aplicaciones críticas, datos personales sensibles, o información confidencial fuera de entornos de red. |
| (Registro de Eventos) | Se deben generar registros de excepciones y eventos relevantes de seguridad en los sistemas y activos, los cuales deben almacenarse un periodo acordado para investigación y control de acceso. |
| (Monitorear el Uso del Sistema) | Debe haber procedimientos para el monitoreo del uso correcto de los activos y el adecuado comportamiento de los sistemas. Los usuarios sólo deben hacer las actividades para las cuales están explícitamente autorizados. |
| (Sincronización de Relojes) | Cuando los sistemas de cómputo o telecomunicaciones operen con relojes en tiempo real se debe acordar un estándar de tiempo y horario. Esto ayuda a la revisión de registros y auditoría. |

| | |
|---|---|
| (Dispositivos Móviles Internos) | Se debe considerar el trabajo externo a través de dispositivos móviles (por ejemplo, netbooks, laptops, tablets, smartphones) proporcionados a los usuarios por la organización. Esto incluye capacitación sobre la responsabilidad y medidas de seguridad relacionadas a su uso y las consecuencias de su pérdida. Asimismo, limitar y ajustar el uso de dispositivos móviles a las condiciones de seguridad y protección de datos de la organización, previamente autorizadas. |
| (Dispositivos Móviles Externos) | Deben existir mecanismos para la incorporación de dispositivos personales ingresados por los usuarios al entorno de la organización, así como para el tratamiento de datos a través de dichos dispositivos. Se debe limitar y ajustar el uso de dispositivos móviles a las condiciones de seguridad y protección de datos de la organización, previamente autorizadas. En su caso, los dispositivos que interactúen con los activos de la organización deberán reforzarse, si un dispositivo no puede acoplarse a los sistemas de información o genera una vulneración, deberá excluirse. |
| (Almacenamiento Privado Dentro del Entorno de Operación) | Se deben establecer reglas para limitar el uso de servicios privados de los usuarios (por ejemplo, el uso de la cuenta de correo electrónico gratuita) para evitar el almacenamiento o transferencia no autorizados de datos personales. Se debe procurar exclusivamente el uso de servicios dentro de entornos empresariales o en los cuales exista un contrato con el prestador del servicio, siempre dentro de las condiciones de las políticas de seguridad de datos personales establecidas en la organización. |
| (Teletrabajo) | En su caso, se deben especificar las condiciones de seguridad y procesos relacionados al teletrabajo, como el robo de equipos, las conexiones seguras, cláusulas de confidencialidad, etc. |
| **Desarrollo y Mantenimiento de Sistemas** | |
| (Validación de Datos de Entrada) | Cuando se proporcionen datos a un sistema, se debe validar que estos sean ingresados de forma correcta, tal que no produzcan conflictos de tratamiento posteriores. En el caso de aplicaciones, se debe asegurar que los métodos de entrada sean seguros y no produzcan vulnerabilidades. |
| (Autenticación de Mensajes) | En los sistemas de información deben existir mecanismos de autenticación de mensajes para asegurar que un mensaje proviene de una fuente autorizada o que no está corrompido. |
| (Validación de Datos de Salida) | En el caso de aplicaciones se debe asegurar que los datos entregados sean los esperados y que se proporcionen en las circunstancias adecuadas. |
| (Cifrado) | Deben existir reglas que definan el uso de cifrado en comunicaciones y/o almacenamiento, así como de los controles y tipos de cifrado a implementar. Se debe identificar la sensibilidad de los datos y el nivel de protección necesario para aplicar el cifrado correspondiente, en almacenamiento y/o transferencia de información. |
| (Firmas Electrónicas) | Se pueden utilizar firmas electrónicas o digitales para ayudar a la autenticidad e integridad de documentos electrónicos. |
| (Servicios de No Repudio) | Es un servicio de seguridad que permite probar la participación de las partes involucradas en una comunicación. Se deben gestionar las disputas que puedan surgir de negar o afirmar la participación de alguien en un evento o acción. |
| (Control de Software y Sistemas) | Se deben tener controles y procesos para integrar software al ambiente operacional, para minimizar el riesgo de corrupción de datos. Se debe probar cualquier cambio o actualización de sistemas críticos antes de |

| | |
|---|---|
| | implementarse en la organización. Se deben aplicar los cambios a una copia concreta del software original y evaluar su funcionamiento. |
| (Protección de Datos de Prueba del Sistema) | Se debe vigilar y gestionar los datos que se utilicen para fines de prueba, evitando el uso de bases de datos con datos personales para tales propósitos, si es necesario usar datos personales, se deben desvincular de su titular antes de usarse. |
| (Control de Acceso a Software de Configuración) | Se debe restringir el acceso a los usuarios no especializados a las carpetas que mantienen la configuración de las aplicaciones o sistemas como las librerías, con el fin de prevenir corrupción en los archivos o software. |
| (Canales Encubiertos y Código Malicioso) | Se deben tener mecanismos para asegurar que con nuevas actualizaciones no se introduzcan canales de comunicación para virus y código malicioso. |
| (Contratación de Servicios de Software) | Se debe tener bien definido y actualizado el arreglo de contratación de servicios de software como pueden ser las licencias de uso, pruebas antes de instalación, requerimientos del sistema, detección de virus y código malicioso, etc. |
| (Procedimientos para el Manejo de Incidentes) | Deben existir procedimientos para el manejo de incidentes, tal que la respuesta sea pronta y efectiva, llevando a cabo un registro para diferenciarlos, de manera que posteriormente se puedan conducir revisiones y comparaciones. |
| (Procedimientos de Acción en caso de Incidente) | Deben existir procedimientos relacionados al monitoreo, reporte, mitigación y documentación de un incidente de seguridad, tal que se pueda verificar la ocurrencia de una vulneración para darle un adecuado seguimiento e implementar las medidas de seguridad correctivas. |
| (Reporte de Incidentes de Seguridad) | Debe existir una manera formal de reportar incidentes de seguridad de acuerdo a la cadena de mando establecida. |
| (Reporte de Fallas en Funcionamiento) | Debe existir una manera formal de reportar fallas en funcionamiento de hardware y/o software de acuerdo a la cadena de mando establecida. |
| (Procedimientos de Notificación de Vulneraciones de Seguridad a Titulares) | Deben existir procedimientos relacionados a la notificación de vulneraciones a los titulares cuando éstas afecten sus derechos patrimoniales o morales. Estos procedimientos deben contemplar la magnitud de la vulneración y los mecanismos que se deban poner a disposición de los afectados. |
| (Aprendizaje de Incidentes) | Cuando aplique, establecer mecanismos para monitorear el tipo, volumen y costo de los incidentes de seguridad. |
| (Procedimientos de Revisión y Actualización) | Deben existir procedimientos de revisión y actualización de las medidas de seguridad una vez mitigada la vulneración a la seguridad para mejorar. |

En caso de que ocurra una vulneración a la seguridad, el responsable o encargado, deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso, a efecto de evitar que la vulneración se repita.

| **Acciones Preventivas y Correctivas** | **Contempladas a Realizar en el Plan de Trabajo** |
|---|---|
| (Complementar el inventario de información) | X |
| (Reforzar la propiedad y devolución de la información) | X |
| (Robustecer la clasificación de la información) | X |

| | |
|---|---|
| (Fortalecer el etiquetado y manejo de información) | X |
| (Regularizar la eliminación de medios) | X |
| (Reforzar los medios físicos en tránsito) | X |
| (Robustecer el control de acceso) | X |
| (Mejorar la gestión de acceso de usuarios con privilegios especiales) | X |
| (Fortalecer la gestión y uso de la información secreta de autenticación) | X |
| (Consolidar las políticas y procedimientos de intercambio de información) | X |
| (Actualizar los acuerdos de confidencialidad) | X |
| (Robustecer la protección de los datos de prueba) | X |
| (Mejorar la continuidad de la seguridad de la información y la disponibilidad de los recursos) | X |
| (Afianzar la protección de los registros) | X |
| (Revisar la seguridad de la información que contenga datos personales) | X |
| (Fortalecer la protección y privacidad de la información personal) | X |
| (Reforzar las acciones relacionadas con el destino final de los datos) | X |
| (Fortalecer la puesta a disposición del aviso de privacidad) | X |
| (Medidas Compensatorias) | X |
| (Borrado Seguro de la Información) | X |
| (Otros. - Especificar) | X |

**6.- MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD**

| **Bitácora de las Vulneraciones a la Seguridad** | | | |
|---|---|---|---|
| **Descripción de la Vulneración de Seguridad** | **Fecha en la que Ocurrió** | **Motivo de la Vulneración** | **Acciones Correctivas Implementadas de Forma Inmediata y Definitiva** |
| (La pérdida o destrucción no autorizada)<br><br>(El robo, extravío o copia no autorizada)<br><br>(El uso, acceso o tratamiento no autorizado)<br><br>(El daño, la alteración o modificación no autorizada) | (Día, Mes y Año) | (Relacionado con las Vulnerabilidades Existentes) | (Especificar) |

| **Informe de Vulneración al Titular** | | | | |
|---|---|---|---|---|
| **Naturaleza del Incidente** | **Datos Personales Comprometidos** | **Recomendaciones al Titular acerca de las medidas que se puedan adoptar para** | **Acciones correctivas realizadas de forma inmediata** | **Medios donde puede obtener más información al respecto** |

| | | | | |
|---|---|---|---|---|
| | | **proteger sus intereses** | | |
| (Especificar) | (Especificar) | (Especificar) | (Especificar) | (Especificar) |

| **Medidas de Seguridad Adoptadas por el Área Responsable** | |
|---|---|
| Riego Inherente a los Datos Personales Tratados | (Nivel de Riesgo Inherente (Bajo, Medio, Alto, Reforzado) |
| Sensibilidad de los Datos Personales Tratados | (Tipo de Datos Personales) |
| Desarrollo Tecnológico | (Si aplica o no aplica, y en su caso, señalar el desarrollo tecnológico) |
| Posibles Consecuencias de una Vulneración para los Titulares | (Describir) |
| Transferencias de Datos Personales que se Realicen | (De ser el caso, señalar a quienes se realizan transferencia de datos personales) |
| Número de Titulares | (Número) |
| Vulneraciones Previas Ocurridas en los Sistemas de Tratamiento | (De ser el caso, describir si hubo vulneraciones previas en los Sistemas de Tratamiento) |
| Riesgo por el Valor Potencial Cuantitativo o Cualitativo que pudieran tener los Datos Personales Tratados para una Tercera Persona No Autorizada para su Posesión | (En su caso, señalar tanto de forma cuantitativa como cualitativa) |

## 7.- PROGRAMA GENERAL DE CAPACITACIÓN

Se diseñará y aplicará diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

## ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

| **Evento por el cual se Actualiza el Documento de Seguridad** | | | |
|---|---|---|---|
| **Se produjeron modificaciones sustanciales al tratamiento de datos personales que derivan en un cambio en el nivel de riesgo** | **Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión** | **Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida** | **Implementación de acciones correctivas y preventivas ante una vulneración de seguridad** |
| X | X | X | X |