Medidas de seguridad en los datos personales

INAI. (2015). Medidas de seguridad en los datos personales

e-uaem Espacio de Formación Multimodal

Módulo 4. Medidas de seguridad en los datos personales

Lic. Oscar Adrián Sánchez Martínez

4.1 Marco de referencia.

El desarrollo del tratamiento automatizado de datos, permite la transmisión de enormes cantidades de ellos en segundos a través de las fronteras nacionales e internacionales, ha hecho que sea necesario considerar la protección de la intimidad en relación a los datos personales.

A lo largo de los módulos anteriores se ha explicado la importancia del derecho a la protección de datos personales, que en términos generales busca impedir vulneraciones de derechos humanos fundamentales, tales como el almacenamiento ilícito de datos personales, exactos o inexactos, o el abuso o la revelación no autorizada de los mismos.

Para lograr una efectiva protección de datos, y más allá del andamiaje jurídico o normativo que se construya para su aplicación, resulta necesario incorporar una serie de medidas técnicas o tecnológicas que coadyuven a garantizar la privacidad y seguridad de los datos personales en el ámbito de los sistemas computacionales.

Las medidas de seguridad para la protección de datos personales, se concentran principalmente en mecanismos, sistemas y metodologías de índole informático que facilitan el cumplimiento de los principios básicos de la protección de datos personales así como de la legislación nacional existente o servir como mejores prácticas comerciales en aquellos países que todavía no dispongan de ella.

Dichas medidas generalmente se van implementando conforme las necesidades del mercado, la irrupción de nuevas tecnologías o herramientas y generalmente no se encuentran supeditadas a la legislación nacional de un Estado en concreto, es decir, son ampliamente aceptadas en el sector con base a su certidumbre y eficacia.

En el caso de México la Ley Federal de Protección de Datos Personales en Posesión de los Particulares dicta que los responsables de los tratamientos de datos personales deben establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

4.1.1 La seguridad de la información en el contexto de los principios de protección de datos.

Las medidas de seguridad en el contexto de datos personales buscan proteger en todo momento tres aspectos del ser humano: Confidencialidad, Privacidad, Derecho a la intimidad.

Dependiendo de la zona geográfica, regulación o contexto académico en el ámbito de la protección de datos, se utilizan estos términos de forma indistinta. Veamos cuáles son sus diferencias:

- El término privacidad es muy usado en informática ya que deriva de una mala traducción del término inglés *privacy*. En castellano, el término legal que refleja este aspecto es la intimidad o derecho a la intimidad.
- El derecho a la intimidad es el derecho que tienen las personas de poder excluir a las demás personas del conocimiento de su vida personal y la facultad para determinar en qué medida esa información sobre su vida personal puede ser comunicada o tratada por otras personas.

En el campo del derecho, es obligado ubicar el concepto PRIVACIDAD que en 1888, el juez norteamericano Tomas Cooley acuñó en torno al “derecho a ser dejado solo, a ser dejado en paz” Definición retomada por el Tribunal Supremo de los Estados Unidos en “*The right to privacy*” en la cual se fundamente la mayor parte de la regulación en las naciones de *common law*.

De la misma forma, el concepto de autodeterminación (*self-determination*) que acuñó el Tribunal Constitucional de Alemania en 1983, sobre el Censo de población consideró también este principio.

La privacidad libertad para elegir que se desea comunicar, cuándo y a quién, manteniendo el control personal sobre la propia información (Alan F. Westin)

De acuerdo a lo anterior, entendemos por intimidad, la libertad del individuo a decidir cuánto sobre sí mismo quiere que sea revelado a otros, cuándo y a quiénes. Se trata por tanto de un derecho a la "propiedad personal" y puede ser entendido como un estado del individuo.

Paralelamente a éste, surge el concepto de confidencialidad, como el deseo de un determinado individuo por restringir el acceso a información personal que puede ser utilizada para determinados fines o propósitos. En contraste con la anterior definición, la confidencialidad puede ser vista como un estado de la información y los datos y no del individuo en sí mismo.

Las Directrices relativas a la protección de la intimidad y de la Circulación transfronteriza de datos personales adoptadas por la Organización para la Cooperación y Desarrollo Económicos (OCDE) se convierten en uno de los principales instrumentos internacionales que permiten la adopción de mecanismos de protección de datos personales.

Algunos de los principios que señalan las directrices de la OCDE, fundamentan la mayor parte de las principales medidas de seguridad que son adoptadas o implementadas por empresas u organizaciones en el mundo.

En este contexto explicaremos brevemente los principios básicos de aplicación nacional que recomienda la OCDE y que se encuentran estrechamente con la implementación de medidas de seguridad:

- **Principio de calidad de los datos**
  8. Los datos personales deberían ser pertinentes a los efectos para los que se vayan a utilizar y, en la medida necesaria a tales efectos, deberían ser exactos y completos, y mantenerse al día.
- **Principio de salvaguardas de seguridad**
  11. Los datos personales deberían protegerse, mediante salvaguardas de seguridad razonables, frente a tales riesgos como pérdida de los mismos o acceso, destrucción, uso, modificación o revelación no autorizados.
- **Principio de responsabilidad**
  14. El controlador de datos debería ser responsable del cumplimiento de las medidas que den efecto a los principios expuestos más arriba.

Al analizar los principios anteriores que recomienda la OCDE, se podría aseverar que sin el uso de herramientas o sistemas informáticos, resultaría prácticamente imposible dar cumplimiento a las directrices 8, 11 y 14.

Dichos principios se pueden desagregar, incorporando los aspectos que protegen de los datos personales:

Calidad de datos	Salvaguardas de seguridad	Responsabilidad
•Disponibilidad (oportunidad) •Consistencia	•Integridad •Confidencialidad	•Control

Estos aspectos o activos de información que protegen los principios antes descritos, son esenciales para la seguridad de la información y se pueden describir de la siguiente manera:

- Confidencialidad. La información sólo puede ser accedida por aquel que esté autorizado.
- Integridad. La información no puede ser eliminada o modificada sin permiso.

- Disponibilidad. La información tiene que estar disponible siempre que sea necesario, evitando por tanto, ataques externos que puedan reducir esta disponibilidad o incluso una caída del servicio.
- Consistencia. Asegurar que las operaciones que se realizan sobre la información se comporten de acuerdo a lo esperado. Esto implica que los programas realicen correctamente las tareas encomendadas.
- Control. Es importante regular y controlar el acceso a la información.

4.1.1.1 Análisis de la normatividad y mejores prácticas internacionales.

Es complejo distinguir conceptualmente privacidad e intimidad pues son conceptos que se encuentran estrechamente relacionados. Sin embargo han sido prácticamente reconocidos en todos los instrumentos internacionales que reconocen la existencia de derechos fundamentales:

1948	**Art. 12 Declaración Universal de los derechos humanos**
	Art. V Declaración Americana de los Derechos y Deberes del Hombre
1950	**Art. 8 Convenio para la protección de los derechos y las libertades fundamentales**
1966	**Art. 17 Pacto Internacional de los derechos civiles y políticos**
1969	**Art. 11 apartado 2 de la convención americana de derechos humanos**

Por su parte este concepto también es recogido en las principales constituciones de diversos países, veamos algunas:

PAIS	ORDENAMIENTO
MÉXICO	Arts. 6, 7 y 16
COLOMBIA	Arts. 15, 20 y 31
BRASIL	Art. 5
ECUADOR	Arts. 23 y 81
ESTADOS UNIDOS	Enmienda IV
VENEZUELA	Art. 60
PERU	Art. 5
ESPAÑA	Art. 18 apartado 3

A continuación se describen algunos de los instrumentos internacionales donde se señalan obligaciones y derechos relacionados con la privacidad y protección de la intimidad.

- Directrices de la OCDE 1980
- Convenio 108 1981
- Resolución 45/95 de la ONU 1990
- Directiva 95/46/CE 1995
- Carta de derechos fundamentales de la unión europea 2000
- Marco de privacidad de APEC 2004
- Directrices de armonización de la red iberoamericana 2007
- Estándares internacionales 2009

En el caso de México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece 8 principios de la protección de datos que se explican brevemente a continuación:

1. **Licitud**. El tratamiento debe ser con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional.
2. **Consentimiento**. El responsable deberá obtener el consentimiento para el tratamiento de los datos personales, a menos que no sea exigible por ley.
3. **Información**. El cumplimiento de este principio se da con un correcto y actualizado Aviso de Privacidad. El aviso de privacidad deberá caracterizarse por ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento
4. **Calidad**. Se cumple con el principio de calidad cuando los datos personales tratados sean exactos, completos, pertinentes, correctos y actualizados, según se requiera para el cumplimiento de la finalidad para la cual son tratados. Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular, y hasta que éste no manifieste y acredite lo contrario, o bien, cuando el responsable cuente con evidencia objetiva que los contradiga. Para cumplir con este principio, el responsable podría implementar un mecanismo para habilitar al titular de los datos personales a modificarlos.
5. **Finalidad**. Es importante distinguir para qué se necesita cada dato personal ya que el tratamiento debe limitarse al cumplimiento de las finalidades previstas en el Aviso de Privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular. Entre las finalidades se

deben incluir, en su caso, las relativas al tratamiento para fines mercadotécnicos, publicitarios o de prospección comercial.

6. **Lealtad**. El principio de lealtad establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad. Ésta es entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordado.
7. **Proporcionalidad**. Sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido. El responsable deberá realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios de acuerdo con la finalidad del tratamiento que tenga lugar.
8. **Responsabilidad**. El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano. Para cumplir con esta obligación, el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines.

De los principios anteriores, y de acuerdo al enfoque de estudio del presente modulo, el principio de responsabilidad es el eje que articula y vela por el cumplimiento de todos los principios establecidos en la ley a cargo del responsable, donde éste debe adoptar o valerse de cualquier mecanismo para garantizar la protección de los datos personales del titular.

Para lo cual es importante también tener en cuenta que, sin mecanismos y/o medidas de seguridad no se puede concebir la protección de los datos personales, razón por la cual se expone en el siguiente cuadro los principales estándares, lineamientos y normas reconocidas a nivel internacional que coadyuvan en la observancia y aplicación del principio de responsabilidad.

Principio de responsabilidad: estándares, lineamientos y normas	Medidas de seguridad o del principio de responsabilidad que contempla
OCDE Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980)	Se contemplan los mismos principios establecidos en México: de limitación de recogida, de calidad de los datos, de especificación del propósito, de limitación de uso, de salvaguarda de la seguridad, de transparencia, de participación individual y de responsabilidad.
OCDE Declaración ministerial sobre la protección de la intimidad de las redes globales (1998)	Mediante este documento, los Estados miembros se obligan a fomentar la confianza en las redes globales y evitar restricciones innecesarias a los flujos transfronterizos de datos personales, comprometiéndose poner en práctica la adopción de políticas sobre la intimidad por medios jurídicos o bien de autorregulación, administrativos o tecnológicos, así como la promoción de la educación y concienciación de los usuarios con respecto a las cuestiones relacionadas con la intimidad en línea y los medios disponibles.
APEC Marco de privacidad 2004	Este instrumento establece el Marco regulatorio en materia de Protección de Datos Personales para los Estados miembro, los cuales,

	a su vez, se comprometen a hacerse responsables de cumplir con los requerimientos locales de protección de datos, así como con todas las leyes aplicables.
Estándares Internacionales sobre Protección de Datos Personales y Privacidad, Resolución de Madrid, 2009	Se protegen los mismos principios en materia de Protección de Datos Personales y ejercicio de Derechos Arco que en México, con base en la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos pero se establecen, además, las reglas de transferencias internacionales, destacando que éstas sólo se podrán dar si el Estado receptor cumple con el nivel de protección establecido como mínimo, mediante cláusulas contractuales o normas internas de privacidad.
Red Iberoamericana de Protección de Datos. Directrices para la armonización de la protección de datos en la comunidad iberoamericana, 2008	Se establecen los principios, derechos y obligaciones, que deberá contener toda Ley nacional en materia de Protección de Datos Personales, de los Estados que formen parte de la comunidad iberoamericana, mismos que ya han sido implementados en la Ley Federal de Protección de Datos Personales en posesión de particulares y su respectivo Reglamento.
Control Objectives for Information and Related Technology (COBIT 5).	Establece objetivos de control para implementar un modelo de Gobernabilidad corporativa. Su aportación en materia de protección de datos es el establecimiento de objetivos de control y mecanismos de monitoreo para el cumplimiento de dichos objetivos, que den a la alta dirección visibilidad sobre el cumplimiento de políticas y lineamientos organizacionales
ITIL, Information Technology Infrastructure Library.	Establece las mejores prácticas para la Gestión de Servicios de TI. En materia de protección de datos personales permitiría establecer lineamientos para el tratamiento legítimo de los datos personales, basado en un Acuerdo de Niveles de servicio y establecimiento de procedimientos para atención de derechos ARCO.
ISO/IEC 27000	Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información de acuerdo a la metodología denominada “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar)
ISO / IEC 27001:2013.- Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013.	Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones.
ISO / IEC 27002:2013.- Publicada desde el 1 de Julio de 2007	Es el nuevo nombre de ISO 17799:2005. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.
ISO / IEC 27003:2010.- Publicada el 01 de Febrero de 2010.	Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.
ISO / IEC 27005:2011.- Publicada en segunda edición el 1 de Junio de 2011.	Proporciona las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
ISO / IEC 27010:2012.- Publicada el 20 de Octubre de 2012.	Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. La ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de información sensible, tanto en organizaciones públicas como privadas, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores.
ISO/IEC 27018: 2014.- Publicada el 29 de Julio de 2014.	Es un código de buenas prácticas en controles de protección de datos para servicios de computación en la nube.

4.1.2 Obligaciones de los responsables en materia de seguridad de datos personales.

El principio de responsabilidad se encuentra plasmado al día de hoy en el artículo 144 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, disposición que señala lo siguiente:

> *Artículo 14.- El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por esta Ley, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.*

De lo anteriormente expuesto se desprende que, el principio de responsabilidad, aunque forma parte de los ocho principios de protección de datos y pareciere que no existe una jerarquía entre los mismos, este principio sí tiene una mayor trascendencia en virtud de ser el eje rector que obliga al responsable del tratamiento a garantizar de forma integral la protección de los datos personales de los titulares.

En relación al Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, el principio de responsabilidad se aborda en los artículos 47 y 48, de los cuales se desprende la obligación del responsable de velar y responder por el tratamiento de los datos personales que realice, o por aquéllos que haya comunicado a un encargado (en territorio mexicano o extranjero). Asimismo, se establece la obligación de adoptar cualquier mecanismo o medida necesaria para velar y responder por dicho tratamiento.

En síntesis podemos señalar que el responsable adquiere el cumulo de todas las obligaciones establecidas en la regulación de la materia, y cuando éste hace uso de un encargado para el tratamiento, éste deberá realizar el tratamiento en los mismos términos que lo hace el responsable. De cambiar la finalidad de la información personal o efectúe una transferencia, incumpliendo las instrucciones del responsable, el encargado adquiere todas las obligaciones de éste en los términos de la Ley, el Reglamento y las disposiciones que les resulten aplicables.

4.2 Fundamentos de la seguridad de datos personales.

La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

Como se ha expuesto anteriormente, la implementación de medios de protección o seguridad de la información en el contexto de la protección de datos personales está enfocada a cumplir los siguientes postulados:

- Se debe evitar la pérdida irremediable de los datos. (INTEGRIDAD Y DISPONIBILIDAD)
- El procesamiento o tratamiento de la información no debe permitir errores. (CONSISTENCIA)
- La información no debe sufrir alguna alteración si no está autorizada. (CONFIDENCIALIDAD)

Resulta necesario considerar otros aspectos o cuestiones relacionados con la seguridad informática.

- Cumplimiento de las regulaciones legales aplicables a cada sector o tipo de organización, dependiendo del marco legal de cada país.
- Control en el acceso a los servicios ofrecidos y la información guardada por un sistema informático.
- Control en el acceso y utilización de archivos protegidos por la ley, contenidos digitales con derechos de autor, archivos con datos de carácter personales, etcétera.
- Identificación de los autores de la información o de los mensajes.
- Registro del uso de los servidores de un sistema informático, etcétera.

Los artículos 47 y 48 del Reglamento de la LFPDPPP establecen las medidas administrativas, técnicas y físicas que seden llevar a cabo para implementar la metodología del análisis de riesgos de seguridad en el tratamiento de los datos personales.

Para la implementación de medidas de seguridad de datos personales resulta primordial para la organización la implementación de herramientas, aplicaciones e infraestructura tecnológica, que les permita incrementar la eficiencia de los procesos y dado que éstos recursos están involucrados en el tratamiento de datos personales, es necesario contar con un inventarios de los recursos tecnológicos, que permitan identificar los riesgos de seguridad, con la finalidad de establecer controles que mejoren las condiciones en que actualmente se encuentran los datos personales.

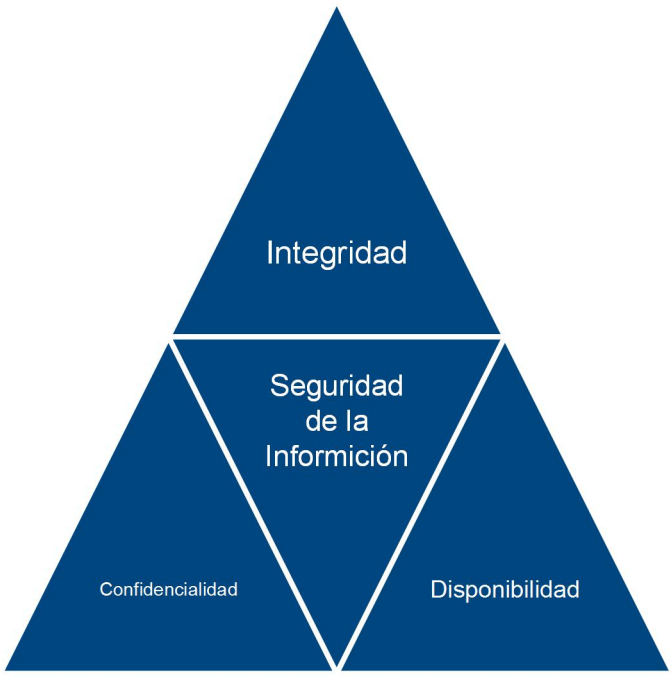
El soporte de la metodología para el análisis de riesgos de seguridad en datos personales está integrado por los siguientes elementos:

- Cumplimiento: Considera todo el conjunto de leyes, regulaciones, normas y estándares que para la prestación del servicio y con base al sector al que pertenezca la organización apliquen.
- Política de Gestión de Datos Personales: Es necesario que la organización cuente con una política avalada y apoyada por la alta dirección, en la cual se establezca el compromiso de la organización para cumplir con la legislación en materia de protección de datos personales.
- Conocimiento: Un factor indispensable para el éxito de las estrategias sobre protección de datos, está relacionado con el grado de conciencia, conocimiento y educación que el personal de la organización tenga sobre el tema, por ello es importante establecer programas de capacitación, realizar campañas de concienciación y educar al personal sobre la importancia de considerar la protección de los datos personales que traten para el desarrollo de sus actividades.

4.2.1 Seguridad de la información.

La definición de seguridad de la información no debe ser confundida con la de «seguridad informática», ya que esta última sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

Desde un punto de vista más amplio, en la norma ISO/IES 17799 se define la Seguridad de la Información como la preservación de su confidencialidad, su integridad y su disponibilidad (medidas conocidas por su acrónimo “CIA” en inglés; “*Confidentiality, Integrety, Availability”*



4.2.1.1 Seguridad informática.

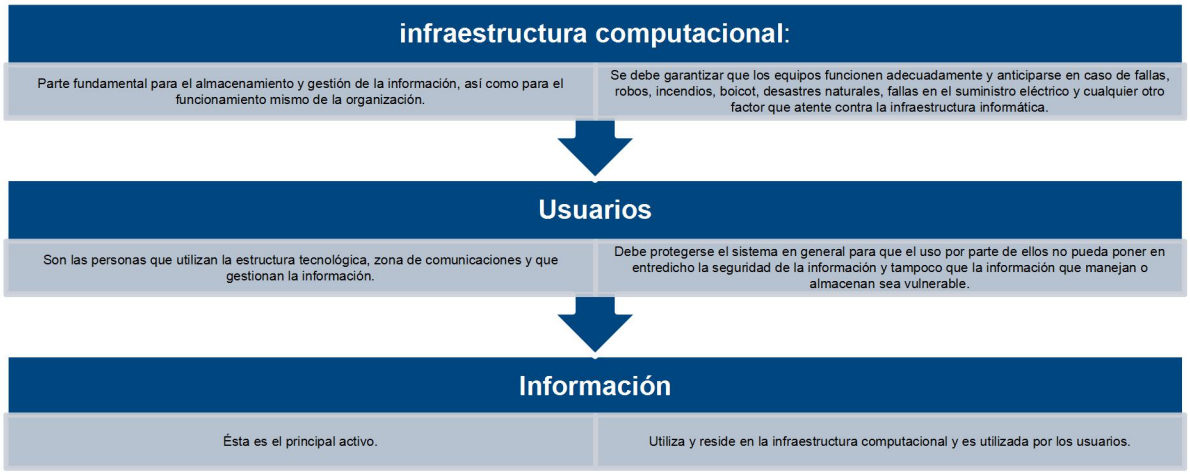
La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática.

Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:



Por su parte, la norma ISO 7498 define la Seguridad informática como “una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una organización”

4.2.2 Vulneraciones de la seguridad.

Vulnerabilidad se define[i] como la evaluación objetiva de la probabilidad de sufrir un determinado ataque un plazo determinado de tiempo.

Para conocer la probabilidad se pueden realizar estadísticas basadas en sucesos pasados elaborados a partir del número de casos favorables y el número de casos posibles.

Vulnerabilidad se usa comúnmente como sinónimo de debilidad, que existe siempre que un ataque es posible, como ejemplo si un equipo informático tiene un error de software que le permita atacarlo de una manera determinada, el equipo entonces presente una debilidad no una vulnerabilidad.

4.2.2.1 Tipos de vulnerabilidades.

El artículo 63 del Reglamento de la LFPDPPP, menciona que existen cuatro tipos de vulneraciones que pueden afectar la seguridad de los datos personales, que son:

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

Algunos ejemplos.

Robo, extravío o copia no autorizada.

- Que se extravíe el equipo de cómputo personal (Laptop) donde almacena los datos personales y que caiga en manos de alguien que pueda hacer una **copia no autorizada** *de la base de datos.*

Perdida o destrucción no autorizada

- Que una persona mal intencionada destruya los archivos físicos o electrónicos que contienen datos personales, lo cual impediría cumplir con la fialidad para la que fueron recabadas, así como atender sus solicitudes de derechos ARCO.

Uso, acceso o tratamiento no autorizado

- Que una persona que usa los datos personales, no bloquee la computadora cuando va al baño, y que como consecuencia, un curioso se acerque y pueda acceder a los archivos.

Daño, alteración o modificación no autorizado.

- Que alguien malintencionado altere lo datos personales de algunos titulares, modifiándolos, lo que impediría cumplir adecuadamente con la fialidad para la que fueron recabadas.

4.2.2.2 Evaluación de riesgos.

Los riesgos de seguridad en los datos personales serán evaluados en función de dos variables:

Impacto

Estimado a partir del volumen de datos personales y la sensibilidad de estos.

Probabilidad de ocurrencia

Consiste en la probabilidad de que ocurra una vulneración de seguridad valuado en función del nivel de exposición y trazabilidad.

Criterios de sensibilidad por dato personal:

NIVEL	SENSIBILIDAD
Muy Alto	Los datos de mayor riesgo son aquellos que de acuerdo a su naturaleza derivan en mayor beneficio para un atacante en caso de obtenerlos, por ejemplo: • Información adicional de tarjeta bancaria (fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal PIN). Titulares de alto riesgo son aquéllas personas que por la profesión o el oficio que desempeñan, tienen una mayor probabilidad de ser atacadas

	debido al beneficio económico o de reputación que sus datos personales pueden representar para un atacante.
Alto	Esta categoría de datos contempla a los datos personales sensibles3, que con base en la LFPDPPP incluyen: • Datos de salud • Filosóficas y morales • Información genética • Afiliación sindical • Origen racial o étnico • Opiniones políticas • Ideología • Preferencia sexual • Creencias religiosas • Hábitos sexuales Cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.
Medio	En esta categoría se incluyen los datos que permiten conocer la ubicación física de la persona, datos patrimoniales, de autenticación con información referente a los usuarios como son las contraseñas, además se incluye en este rubro la información biométrica, los datos jurídicos y de la tarjeta bancaria.
Bajo	Esta categoría incluye los datos de identificación y contacto o información académica o laboral.

4.2.3 Amenazas.

Las amenazas son cualquier circunstancia potencial que pueda afectar los procesos y expectativas de la organización, para proteger esas expectativas se debe identificar, evaluar, y prever que amenazas pueden afectar su cumplimiento y ser capaces de medir, sea cuantitativamente o cualitativamente la posibilidad y probabilidad de materialización de esas amenazas.

4.2.3.1 Tipos de Amenazas.

Las amenazas pueden clasificarse en tres grandes grupos:

- Amenazas terciarias o directas, que son las que amenazan directamente el cumplimiento de nuestras expectativas. Se dividen en tres factores:
    - Ataques. Responden a un actor con determinada motivación, medio y capacidad
    - Accidentes. Suelen ser naturales como puede ser un terremoto o relacionados con fallas físicas o lógicas del hardware por defecto o uso prologado.
    - Errores. Se encuentran principalmente relacionado con defectos de configuración, programación o respuesta del software.

- Amenazas secundarias, Son las que disminuyen o eliminan el grado de éxito de las medidas que ponemos para mitigar las amenazas primarias. Ejemplo. Defectos en cortafuegos.

- Amenazas primarias, Son las que evitan que se mantengan o lleguen a establecerse las medidas que mitigan las amenazas terciarias o secundarias. Ejemplo. Falta de aplicación de procedimientos de seguridad en la organización.

Origen	Motivación	Posible consecuencia
Hacker, cracker	• Desafío • Dinero • Ego • Estatus • Rebelión	• Acceso no autorizado al sistema • Ingeniería social • Intrusión en los sistemas • Robos
Criminal Computacional	• Alteración no autorizada de información • Destrucción de información • Ganancia económica • Revelación ilegal de información	• Acciones fraudulentas, robo • Extorción y chantaje, acoso • Intrusión a los sistemas informáticos • Sobornos de información • Suplantación de identidad • Venta de información personal
Terrorista	• Chantaje • Destrucción • Explotación • Ganancia política • Reconocimiento mediático • Venganza	• Ataque a sistemas (por ejemplo, denegación de servicio) • Manipulación de los sistemas • Penetración a los sistemas • Terrorismo (por ejemplo, bombas)
Espía industrial (inteligencia empresarial, gobiernos extranjeros, robo de tecnología, etc.)	• Espionaje económico • Ventaja competitiva	• Acceso no autorizado a información clasificada o propietaria • Explotación económica • Ingeniería social • Intrusión a la privacidad del personal • Penetración a los sistemas • Robo de información • Ventaja política
Interno (Personal con poco entrenamiento, descontento, negligente, deshonesto o empleados despedidos)	• Curiosidad • Ego • Errores no intencionales u omisiones (por ejemplo, errores de captura de información, errores de programación) • Inteligencia	• Abuso en la operación de los sistemas • Acceso no autorizado a los sistemas • Ataque a empleados • Chantaje • Código malicioso • Consulta de información clasificada o propietaria • Datos incorrectos o corruptos

	• Ganancia económica • Venganza	• Errores en los sistemas • Fraude y robo • Intercepción de comunicaciones • Intrusiones a sistemas • Sabotaje de los sistemas • Sobornos de información • Venta de información personal

4.2.4 Ataques.

Los ataques son incidentes provocados por actores externos o internos, para los efectos de este módulo no nos detendremos en el estudio o clasificación de sus intenciones o motivaciones, sin embargo resulta relevante conocer los posibles recursos y oportunidades que disponen para estimar la dimensión del posible ataque.

Los ataques pueden suceder de forma individual, o utilizarse en conjunto para producir el efecto deseado por un atacante. Por ejemplo, mediante ingeniería social se puede obtener un acceso físico no autorizado que proporcione medios para desactivar medidas de seguridad u finalmente realizar potro ataque o robo de información

Algunos de los tipos de ataques más comunes son:

4.2.4.1 Espionaje.

Consiste en el acceso ilegitimo sea físico o lógico, a la información mensajes y servicios de la organización. El objetivo último del espionaje suele ser la revelación de secretos o exposición de datos personales.

El espionaje puede consistir en las siguientes acciones:

- Escuchas
- Lectura o copia de información
- Lectura de mensajes o información cifrados
- Reproducción no autorizada de información
- Análisis de trafico

4.2.4.2 Sabotaje.

Es un ataque destructivo, con el que se intenta producir el máximo daño posible. La protección más efectiva ante esta amenaza es la eliminación de oportunidades y el uso de medidas de reducción del impacto.

El sabotaje puede consistir en las siguientes acciones:

- Interrupción
- Borrado
- Modificación
- Generación malintencionada de información

- Denegación de servicio
- Interrupción de recursos
- Terrorismo

4.2.4.3 Compromiso de medios de autenticación

El compromiso de claves o credenciales es una de la amenazas con consecuencias más serias, debido a que en muchas ocasiones, no sabremos que el compromiso se ha producido. El compromiso de esta medida de seguridad, permite que el atacante pueda suplantar nuestra identidad, adquiriendo la misma capacidad que se tienen dentro de un sistema.

De la misma forma resulta complejo demostrar la no autoría de la acción no autorizada.

4.2.4.4 Ingeniería social

Es una de las amenazas más graves y sencilla de explotar. El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil".

En la práctica, un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Vía Internet o la web se usa, adicionalmente, el envío de solicitudes de renovación de permisos de acceso a páginas web o memos falsos que solicitan respuestas e incluso las famosas cadenas, llevando así a revelar información sensible, o a violar las políticas de seguridad típicas.

Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones, –por ejemplo proporcionando detalles financieros a un aparente funcionario de un banco– en lugar de tener que encontrar agujeros de seguridad en los sistemas informáticos.

4.2.4.5 Fraudes.

Los fraudes consisten en aprovechar los recursos de la organización de forma no legítima. Esto generalmente está enfocado a los sistemas de orden financiero o contable.

El código malicioso también representa una de los ataques más comunes que comprometen la seguridad de la información, es por ello que se abordará más adelante con mayor amplitud.

4.2.5 Código malicioso. (malware)

También llamado *badware*, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

El término malware es muy utilizado para referirse a una variedad de software hostil, intrusivo o molesto.

El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos.

El término malware incluye:

- Virus. Tiene por objetivo alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan Archivos ejecutables por otros infectados con el código de este.
- Gusanos. Se propagan de computadora a computadora, pero a diferencia de un virus, tiene la capacidad a propagarse sin la ayuda de una persona. Lo más peligroso de los worms o gusanos informáticos es su capacidad para replicarse en el sistema informático
- Troyanos. Se presenta como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, brinda a un atacante acceso remoto al equipo infectado. En la mayoría de los casos, crean una puerta trasera que permite la administración remota a un usuario no autorizado
- Rootkits. Permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones.
- Scareware. Abarca varias clases de software para estafar con cargas maliciosas, o con limitados o ningún beneficio, que son vendidos a los consumidores vía ciertas prácticas no éticas de comercialización.
- Spyware. Recopila información y la transmite a una entidad externa sin conocimiento o el consentimiento del propietario. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware.
- Adware. Programa que automáticamente muestra publicidad web al usuario durante su instalación o durante su uso para generar lucro a sus autores. 'Ad' en la palabra 'adware' se refiere a advertisement' (anuncios) en idioma inglés.
- Crimeware. Es un tipo de software que ha sido específicamente diseñado para la ejecución de delitos financieros en entornos en línea.
- Exploit. Es un programa que toma ventaja del hecho de que en la arquitectura actual presenta algún defecto conocido para provocar daños o ganar acceso con derechos de administrador.

4.3 Diseño de un programa de seguridad.

Garantizar la seguridad de la información y en particular de los datos personales que se tratan en una organización requiere de optimizar e integrar medidas de seguridad de la información. Para lograr este propósito, es importante valorar los recursos humanos, materiales, información ´de la organización y las disposiciones legales aplicables.

La ley mexicana define un Sistema de Gestión de Seguridad de Datos Personales como un sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del

riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley, su Reglamento, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.

Un programa de seguridad es un conjunto de elementos mutuamente relacionados o que interactúan por un fin u objetivo. Por lo tanto, un Sistema de Gestión (SG) se define como un conjunto de elementos y actividades interrelacionadas para establecer metas y los medios de acción para alcanzarlas.

Asimismo, un sistema de gestión apoya a las organizaciones en la dirección, operación y control de forma sistemática y transparente de sus procesos, a fin de lograr con éxito sus actividades, ya que está diseñado para mejorar continuamente el desempeño de la organización, mediante la consideración de las necesidades de todas las partes interesadas.

Es importante tomar en cuenta que una organización tiene que definir y gestionar numerosas actividades para funcionar con eficiencia. Estas actividades se convierten en procesos que tienen la característica de recibir elementos de entrada, los cuales se gestionan para regresar al final de su ciclo, como elementos de salida (resultados).

Por ejemplo, un proceso de Auditoría puede recibir como elementos de entrada objetivo, alcance y plan de auditoría, así como el informe de resultados de la auditoría anterior, y como elemento de salida un nuevo informe de auditoría. A menudo, la salida de un proceso se convierte directamente en la entrada del proceso siguiente, y la interconexión entre procesos genera sistemas que se retroalimentan para mejorar. Todos estos recursos deben de estar integrados en un grupo general e interactuar con el entorno de cado uno de los elementos que integran el programa de seguridad.

Estos componentes pueden ser:

- Medidas de seguridad administrativas
- Medidas de seguridad físicas
- Medidas de seguridad técnicas

4.3.1 Medidas de seguridad administrativas.

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

4.3.2 Medidas de seguridad físicas.

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

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

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

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

d) Garantizar la eliminación de datos de forma segura.

4.3.3 Medidas de seguridad técnicas.

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

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

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

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

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

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

a) El riesgo inherente por tipo de dato personal;

b) La sensibilidad de los datos personales tratados;

c) El desarrollo tecnológico, y

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

Además, se debe tomar en cuenta los siguientes elementos:

a) El número de titulares;

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

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

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

Con el fin de establecer y mantener la seguridad de los datos personales debes implementar todas las acciones que se te han recomendado en otras etapas de la implementación de tu estrategia de privacidad.

Adicionalmente se recomienda:

1. Realizar un análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;

2. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivada del análisis de brecha;

3. Llevar a cabo revisiones o auditorías;

4. Realizar un registro de los medios de almacenamiento de los datos personales.

5. Repetir cada año los pasos anteriores.

Actualmente se tiene la opción de contar con un esquema de autorregulación. Según la Ley de México, las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en la materia, que complementen lo dispuesto por ella.

Dichos esquemas deberán contener mecanismos para medir su eficacia en la protección de los datos, consecuencias y medidas correctivas en caso de incumplimiento. Los esquemas de autorregulación podrán traducirse en:

a) códigos deontológicos o de buena práctica profesional,

b) sellos de confianza u otros mecanismos

Estos contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos y facilitar el ejercicio de los derechos de los titulares. Dichos esquemas serán notificados de manera simultánea a las autoridades sectoriales correspondientes y al Instituto.

4.3.4 Administración de la seguridad.

Los responsables de seguridad deben encargarse de detectar las expectativas de la organización, tomar las medidas más rentables para disminuir el riesgo y supervisar el cumplimiento de las responsabilidades de seguridad de aquellas que no desempeñe directamente.

Para lo anterior, los responsables deben de auxiliarse de:

- Política de seguridad
- Normas de seguridad
- Estándares de seguridad
- Procedimientos de seguridad
- Plan de continuidad de operaciones
- Norma de uso aceptable
- Acuerdos de seguridad

4.3.4.1 Implementación de las Medidas de Seguridad Aplicables a los Datos Personales

La organización deberá considerar un conjunto de indicadores para identificar de manera oportuna, cualquier cambio en el contexto de la organización y así mantener una visión general de la imagen del riesgo, entre más pronto se realice esta detección, las partes interesadas podrán tomar decisiones más efectivas para proteger los datos personales.

La naturaleza de los indicadores puede variar dependiendo del tipo de activo. Por ejemplo, vigilar la actitud de un empleado inconforme o que se dejen documentos con información personal en las impresoras o fotocopiadoras. El monitoreo de estos indicadores conllevan una detección temprana de posibles amenazas, y así lograr una respuesta a incidentes efectiva.

Deberá designarse un miembro del equipo del responsable para la rendición de cuentas de la gestión de los datos personales dentro de la organización, de modo que tanto el cumplimiento de la legislación en protección de datos, como la política de gestión y seguridad de datos personales, puedan ser demostrados.

El responsable designado al interior de la organización para la protección de datos personales, en los términos del artículo 30 de la Ley, deberá estar a cargo del cumplimiento de la política en el día a día.

Esta función debe tener, al menos, las siguientes responsabilidades:

a) compromiso total del cumplimiento de la política;

b) desarrollo y revisión de la política;

c) asegurar la implementación de la política;

d) revisiones de la gestión de la política

e) entrenamiento y concienciación necesaria de la política

f) aprobación de procedimientos donde sean tratados los datos personales, como:

- La administración y comunicación de noticias de privacidad;
- manejo de solicitudes de los titulares;
- recolección y manipulación de datos personales;

- manejo de quejas;
- gestión de incidentes de seguridad;
- contratación de servicios externos y prestación;

g) enlace con las personas a cargo del manejo de riesgos y asuntos de seguridad dentro de la organización;

h) provisión de asesoramiento en asuntos ante el INAI y en relación con proyectos que involucren temas de seguridad de los datos personales, como puede ser compartirlos o transferirlos fuera de la organización;

i) interpretación de las exenciones aplicables al tratamiento de los datos personales;

4.3.5 Incidentes de seguridad.

Un incidente de seguridad es cualquier evento que tenga o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras.

Cuando una amenaza se materializa, se tiene un incidente. Algunos incidentes son provocados (ataques), otros se producen por falta de diligencia (errores), y otros son, sobrevenidos (accidentes o catástrofes). Cuando se ha producido un incidente, sea por ataque o no, debemos ser capaces de detectarlo e identificarlo.

El manejo de incidentes es complejo, y aunque existe un interés lógico en la identificación del atacante y la represalias legales.

Un incidente de seguridad puede causar ciertos tipos afectaciones en la organización, tales como:

- Pérdida de información confidencial, afectando la confidencialidad, integridad y disponibilidad de la misma.
- Robo de activos físicos informáticos tales como computadoras, dispositivos de almacenamiento, impresoras.
- Daños a los activos físicos informáticos incluyendo computadoras, dispositivos de almacenamiento, impresoras,
- Denegación de servicio.
- Uso indebido de los servicios, información o activos de información.
- Infección de los sistemas por software no autorizado.
- Intento de acceso no autorizado.
- Cambios no autorizados a la organización de hardware, software, o su configuración.
- Respuesta a las alarmas de detección de intrusos.

En primera instancia se debe enfocar a analizar la probabilidad de que el incidente ocurra nuevamente, identificar la fuente, recolectar evidencias e incluso tomar medidas de respuesta, normalmente legales.

4.3.6 Gestión de incidentes de seguridad.

La gestión de incidentes de seguridad define las pautas de lo que se debe de realizar en caso de incidente de seguridad y obtiene las fases de respuesta a incidentes con el propósito de minimizar los daños, evaluar el incidente, así como las actividades a realizar cuando se presente un incidente y como responder a ello.

Para logran una adecuada gestión de un incidente de seguridad es necesario contar que la organización cuente con un sistema de gestión de seguridad de datos personales, un plan de continuidad de operaciones, un plan de recuperación a desastres o contar con un procedimiento o entidad encargada de atender este tipo de incidentes.

En términos generales y con el propósito de atender incidentes de seguridad de datos personales, este plan de acción de contener cuando menos los siguientes elementos:

1. Políticas y Procedimientos.
    a. Establecer las políticas de Seguridad.
    b. Contar con procedimientos de Respuesta a Incidentes.
    c. Contar con procedimientos de Recuperación y respaldo (backup)
2. Implementar políticas con herramientas de seguridad que incluyen firewalls, sistemas de detección de intrusos, y otros elementos necesarios.
3. Colocar avisos de advertencia contra el uso no autorizado en los puntos de acceso del sistema.
4. Establecer directrices de respuesta considerando y discutiendo posibles escenarios.
5. Capacitación de los usuarios sobre la seguridad y entrenar al personal de TI en el manejo de situaciones de seguridad y el reconocimiento de intrusiones.
6. Debe haber una lista de contactos con los nombres figurando la prioridad de los contactos.
7. Prueba del proceso.

Todos los miembros de una organización deben saber cómo actuar en caso de incidente. El área de TI realizará la mayoría de las acciones en respuesta a un incidente, pero todo el personal debe saber cómo informar de incidentes internamente. Los usuarios finales deben informar de cualquier actividad sospechosa al personal de TI directamente o a través de un personal de asistencia.

Cada miembro del equipo debe revisar el plan de respuesta a incidentes detalladamente. El hecho de que el plan sea fácilmente accesible para todo el personal de TI ayudará a garantizar que, cuando se produzca un incidente, se seguirán los procedimientos correctos.

Para elaborar un plan satisfactorio de respuesta a incidentes se deben tomar en cuenta las siguientes consideraciones:

1. Realizar una evaluación inicial.
2. Comunicar el incidente.
3. Contener el daño y minimizar el riesgo.
4. Identificar el tipo y la gravedad del ataque.
5. Proteger las pruebas.
6. Notificar a los organismos externos, si corresponde.
7. Recuperar los sistemas.
8. Compilar y organizar la documentación del incidente.
9. Valorar los daños y costos del incidente.
10. Revisar las directivas de respuesta y actualización.

Estos pasos no son puramente secuenciales, sino que se suceden a lo largo del incidente. Por ejemplo, la documentación comienza al principio y continúa durante todo el ciclo de vida del incidente; las comunicaciones también se producen durante todo el incidente.

4.3.6.1 Detección de un incidente.

La detección de un incidente puede ocurrir de forma inesperada y por diversos medios, sin embargo de forma regular puede venir de los siguientes medios:

1. Sistema de detección de intrusos (IDS).
2. Un administrador de red de la organización.
3. Un administrador del firewall.
4. Un equipo de monitoreo contratado por la organización.
5. Personal administrativo de la entidad.
6. El departamento de seguridad o una persona de seguridad.
7. Una fuente externa a la entidad.

Muchas actividades podrían indicar un posible ataque. Por ejemplo, cuando un administrador de red realiza labores de mantenimiento del sistema, puede parecer que alguien está iniciando alguna forma de ataque. En otros casos, un sistema mal configurado puede llevar a varios falsos positivos en el sistema de detección de intrusiones, lo que dificulta la identificación de los verdaderos incidentes.

Como parte de su evaluación inicial, debe realizar las siguientes acciones:

1. Tomar medidas para determinar si está tratando con un incidente verdadero o un falso positivo.
2. Hacerse una idea general del tipo y la gravedad del ataque.
3. Debe reunir al menos suficiente información para su investigación adicional y para empezar a contener los daños y minimizar el riesgo.
4. Registrar las acciones minuciosamente. Estos registros se usarán más adelante para documentar el incidente (ya sea real o falso).

Cuando sospeche que hay un incidente de seguridad, se debe comunicar rápidamente la infracción a las pareas responsables. El coordinador de incidentes, junto con el resto del equipo, debe identificar rápidamente con quién debe atender el incidente. Así se garantiza que se puede mantener un control y una coordinación de incidentes adecuada, al tiempo que se minimizan los daños.

4.3.6.2 Análisis de un incidente.

Son muchos los factores que determinarán la respuesta adecuada, lo cual incluye:

1. Real: Seguir los procedimientos respectivos para para eliminar el incidente.
2. Percibido: verificar y analizar si es real para tomar medidas contra él.
3. Buscar medidas mientras se encuentra la solución para detenerla intrusión.
4. Determinar la naturaleza del ataque (puede ser diferente a lo que sugiere la evaluación inicial).
5. Determinar el punto de origen del ataque.
6. Determinar la intención del ataque. ¿Estaba el ataque dirigido específicamente a su organización para conseguir información concreta o fue un ataque aleatorio?
7. Identificar los sistemas puestos en peligro.
8. Identificar los archivos a los que se ha tenido acceso y determinar su grado de confidencialidad.

4.3.6.3 Contención, erradicación y recuperación.

La respuesta a un caso de intrusión debe ser rápida o por lo menos tratar de ejecutar acciones para ganar tiempo para mitigar el incidente.

Si el incidente es detectado por un sistema IDS se generará una alerta de seguridad que deberá a avisar de forma oportuna al personal técnico responsable de su atención.

La contención es el proceso de adoptar medidas para prevenir nueva intrusión o daño y eliminar la causa del problema. Algunas de las actividades que se llevan a cabo en este proceso son las siguientes:

1. Proteger la vida humana y la seguridad de las personas. Por supuesto, esta debe ser siempre la máxima prioridad.
2. Proteger la información secreta y confidencial. Como parte de su plan de respuesta a incidentes, debe definir claramente qué información es secreta o confidencial. Esto le permitirá establecer prioridades a sus respuestas de protección de datos.
3. Proteger otra información, como datos científicos, sobre propiedad o del ámbito directivo. Puede que otra información de su entorno también sea valiosa. Debe proteger en primer lugar los datos más valiosos antes de pasar a otros menos útiles.
4. Proteger el hardware y software contra el ataque. Esto incluye protegerlos contra la pérdida o la modificación de los archivos de sistema y contra daños físicos al hardware. Los daños en los sistemas pueden tener como consecuencia un costoso tiempo de inactividad.

5. Minimizar la interrupción de los recursos informáticos (incluidos los procesos). Aunque el tiempo de producción sea muy importante en la mayoría de los entornos, el hecho de mantener los sistemas en funcionamiento durante un ataque puede tener como consecuencia problemas más graves en el futuro. Por este motivo, la minimización de la interrupción de los recursos informáticos debe ser generalmente una prioridad relativamente baja.

La erradicación consiste en determinar la forma en que ocurrió la intrusión. Fijar la fuente de la intrusión si fue vía correo electrónico por ejemplo, se debe verificar si el ataque sucedió a través de un puerto, a través de servicios, o debido que no se encuentran actualizados sistemas o aplicaciones.

Adicional a lo anterior, tomar medidas inmediatas para evitar una nueva infección:

1. Cerrar los puertos de los servidores que no se encuentren operando.
2. Revisar el sistema que fue afectado para poder tomar medidas frente la intrusión.
3. Volver a instalar el sistema, utilizar las copias de respaldo y asegurar que las copias se hayan realizado antes de la intrusión.
4. Información a los empleados y usuarios de la organización.
5. Desactivar los servicios sin utilizar en el sistema afectado.

La recuperación por su parte, son los procedimientos que se deben seguir para restaurar los sistemas afectados, conservando las pruebas en contra de la intrusión, asegurando de tener respaldos del sistema y que sean del sistema afectado.

La forma de recuperar el sistema dependerá generalmente del alcance de la infracción de seguridad, por lo cual se deberá determinar si puede restaurar el sistema existente dejando intacto todo lo posible, o si es necesario volver a crear completamente el sistema.

Para restaurar los datos se asume, por supuesto, que cuenta con copias de seguridad realizadas antes de que ocurriera el incidente. El software de integridad de archivos puede ayudar a señalar el primer daño en aparecer. Si el software le avisa sobre un archivo modificado, sabrá que la copia de seguridad que hizo antes de la alerta es adecuada y que debe conservarla para su uso cuando vuelva a crear el sistema en peligro.

Un incidente podría dañar los datos almacenados varios meses antes de su descubrimiento. Por lo tanto, es muy importante que, como parte del proceso de respuesta a incidentes, determine la duración del incidente. (El software de integridad del sistema y archivos, junto con los sistemas de detección de intrusiones, puede ayudarle en esta tarea.)

Además de lo anterior, la recuperación de un incidente de seguridad puede incluir las siguientes actividades:

1. Volver a instalar el sistema afectado a partir de cero y la restauración de datos de copias de seguridad si es necesario.

2. Asegurar de conservar las pruebas en contra de la intrusión de copias de seguridad de los registros o, posiblemente, todo el sistema.
1. Los usuarios deben cambiar las contraseñas, si las contraseñas han sido interceptadas e informales que deben ser fuertes y no divulgarlas.
2. Asegurar de que el sistema está completamente actualizada.
3. Asegurar de que la protección antivirus en tiempo real y detección de intrusos se está ejecutando.

4.3.6.4 Identificación del atacante.

Resulta necesario tener en cuenta que los daños pueden producirse de muchas formas y que en el tema de protección de datos personales, un titular en el periódico que describa una vulneración de seguridad puede ser mucho más destructivo que muchas intrusiones en el sistema.

Por este motivo y para evitar que los atacantes estén avisados, sólo se debe informar a aquellos implicados en la respuesta a incidentes hasta que el incidente esté totalmente controlado. Basándose en cada situación concreta, el equipo determinará a quién se debe informar acerca del incidente.

La comunicación externa debe estar coordinada con el representante legal.

Intentar evitar que los atacantes sepan que ya han sido descubiertos puede resultar difícil, porque algunas respuestas esenciales pueden alertar a los atacantes. Por ejemplo, si hay una reunión de emergencia del área informática o solicita un cambio inmediato de todas las contraseñas, algún atacante interno puede saber que está al corriente de un incidente.

Determinar los puntos de acceso usados por el atacante e implementar las medidas adecuadas para evitar futuros accesos. Las medidas pueden incluir la des habilitación de un módem, la adición de entradas de control de acceso en un enrutador o firewall, o el aumento de las medidas de seguridad físicas.

Conforme lo expuesto anteriormente, existe la posibilidad de que el atacante puede ser un empleado, contratista, empleado temporal u otra persona de la organización. Sin documentación completa y detallada, la identificación de un atacante interno será muy difícil. Una documentación apropiada también le proporciona la mejor oportunidad de procesar legalmente a los atacantes.

En muchos casos, si el sistema ha sufrido un ataque intencionado, puede que sea necesario interponer una denuncia contra los autores. Para conservar esta opción, se deben reunir pruebas que se puedan usar contra ellos, incluso si finalmente se decide no llevar a cabo tal acción.

Alguien cualificado en el análisis forense informático debe hacer al menos dos copias de seguridad completas bit a bit del sistema entero con medios totalmente nuevos. Al menos se debe realizar una copia de seguridad en un medio que admita una sola escritura pero múltiples lecturas, como CD-R o DVD-R. Esta copia de seguridad se debe usar sólo para propósitos legales y se debe proteger en lugar seguro hasta que se necesite.

4.3.6.5 Documentación del incidente.

Durante el proceso de gestión del incidente se debe documentar minuciosamente todos los procesos y acciones realizadas, incluyendo una descripción de la infracción y detalles de cada acción tomada (quién llevó a cabo la acción, cuándo lo hizo y por qué motivos). Se debe avisar a todas las personas implicadas con acceso durante el proceso de respuesta.

Después, se debe organizar la documentación cronológicamente, comprobar que está completa, y firmarla y revisarla con la directiva y los representantes legales. Asimismo, deberá proteger las pruebas recopiladas en la fase de protección de pruebas. Debe plantearse la presencia de dos personas durante todas las fases, que puedan aprobar cada paso. Esto ayudará a reducir la probabilidad de que las pruebas se consideren no admisibles y de que se modifiquen después.

Finalmente se debe elaborar un documento sobre los hallazgos del incidente incluyendo la forma en que se produjo la intrusión, cuando se produjo el ataque, la respuesta otorgada y si está fue efectiva.

Adicionalmente se deben realizar las siguientes actividades.

1. Preservación de pruebas. Hacer copias de los registros de intrusión y mantener las listas de testigos.
2. Evaluar los daños y el costo. Evaluar si los daños a la entidad y estimación de costos.
3. Revisión y actualización de políticas de respuesta. Considerar si implementar una política podría haber evitado la intrusión al sistema.
4. Considerar si una política o procedimiento no se siguió, lo que permitió la intrusión y mejorarla.
5. Estudiar si la respuesta al incidente fue la apropiada o no y establecer como se puede perfeccionar.
6. Informar a las partes interesadas.
7. Revisar que todos sistemas estén actualizados, que se estén cumpliendo las políticas para el cambio de contraseñas y que los antivirus se encuentren operando adecuadamente.
8. Se deberán crear políticas de seguridad cada vez que el administrador lo estime necesario para evitar una intrusión al sistema.

La LFPDPPP especifica en su artículo 20 que las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento de datos personales y que afecten de forma significativa los derechos patrimoniales o morales de los titulares deberán ser informadas inmediatamente por el responsable al titular, a fin que este último tome las medidas pertinentes en la defensa de sus derechos.

4.3.7 Normas internaciones.

Con relación a la implementación de sistemas de seguridad de información y en específico sobre la administración de riesgos e incidentes así como de la continuidad del negocio, la Organización Internacional de Normalización (ISO) ha desarrollado una serie de normas que al igual que las otras que ha publicado, buscan facilitar el comercio internacional a través de la implementación de especificadores de productos, servicios y sistemas que garanticen calidad, seguridad y eficiencia.

- ISO / IEC 27005:2011.- Publicada en segunda edición el 1 de Junio de 2011. No es certificable. Proporciona las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
- ISO/IEC 27031: 2011.- Publicada el 01 de Marzo de 2011. No es certificable. Se trata de una guía de apoyo para la adecuación de las tecnologías de información y comunicación de una organización para la continuidad del negocio.
- ISO/IEC 27032: 2012.- Publicada el 16 de Julio de 2012. Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas. Cubre las prácticas de seguridad a nivel básico para los interesados en el ciberespacio. Esta norma establece una descripción general de Seguridad Cibernética.
- ISO/IEC 27035: 2011.- Publicada el 17 de Agosto de 2011. Proporciona una guía sobre la gestión de incidentes de seguridad en la información. Consta de 3 partes adicionales actualmente en fase de desarrollo.

Para la implementación de estas acciones y en general del Sistema de Gestión de Seguridad de Datos Personales, el INAI México recomienda la consulta de los siguientes estándares internacionales, en los que se basan las Recomendaciones:

- BS 10012:2009, Data protectionSpecification for a personal information management system.
- ISO/IEC 27001:2005, Information TechnologySecurity techniquesInformation security management systems Requirements.
- ISO/IEC 27002:2005, Information TechnologySecurity techniquesCode of practice for security management.
- ISO/IEC 29100:2011, Information technologySecurity techniquesPrivacy framework.
- ISO 31000:2009, Risk managementPrinciples and guidelines.
- ISO GUIDE 72, Guidelines for the justification and development of management systems standards.
- ISO GUIDE 73, Risk managementVocabulary.
- ISO 9000:2005, Quality management systemsFundamentals and vocabulary.

- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems.
- OECD Guidelines for the Security of Information Systems and NetworksTowards a Culture of Security.

4.4 Casos de vulneración.

4.4.1 Caso Sony (Estados Unidos).

- http://www.cnnexpansion.com/tecnologia/2011/05/06/sony-se-disculpa-por-fallas-de-seguridad
- http://www.cnnexpansion.com/tecnologia/2011/05/09/ifai-pide-datos-a-sony-mexico-por-ataque
- http://mexico.cnn.com/tecnologia/2011/06/02/un-nuevo-ataque-informatico-a-sony-expone-datos-de-un-millon-de-clientes

4.4.2 Caso Inteco (España).

- http://www.red.es/redes/sala-de-prensa/nota-de-prensa/inteco-informa-sobre-el-robo-de-datos-de-su-plataforma-de-formacion-on
- https://www.incibe.es/file/vuiNP2GNuMinSjvyZnPW2w
- http://www.europapress.es/portaltic/sector/noticia-inteco-sufre-robo-datos-afecta-20000-usuarios-20110607103547.html

4.4.3 Caso Banorte (México).

- http://www.elfinanciero.com.mx/economia/roban-datos-de-clientes-de-banorte.html
- http://www.20minutos.com.mx/noticia/27214/0/banorte-sufre/robo-de-datos/cuentahabientes/
- http://www.periodismolibre.com.mx/products/sancionan-a-banorte-por-mal-uso-de-datos-personales/

4.5 Medidas de seguridad recomendadas.

En caso de vulneraciones, la Ley obliga a informar al titular sobre las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto sea confirmado que ocurrió la vulneración y se hayan tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes.

Se debe preparar la siguiente información:

1. La naturaleza del incidente;
2. Los datos personales comprometidos;
3. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
4. Las acciones correctivas realizadas de forma inmediata, y
5. Los medios donde puede obtener más información al respecto.

Recuerda que en caso de que ocurra una vulneración a los datos personales, debes analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita. Es por eso que se insiste en la importancia de las auditorías periódicas, por lo menos una vez al año.

La organización deberá elegir los controles administrativos, técnicos o físicos que le permitan atender de mejor manera los riesgos identificados y minimizar las consecuencias de posibles vulneraciones.

La siguiente tabla de controles de seguridad elaborada por el INAI México se puede usar como referencia en la elaboración del plan de tratamiento del riesgo, en la valoración del riesgo, o incluso para establecer el contexto de seguridad de la organización en función de la presencia o ausencia de los controles siguientes:

Objetivo de Control	Descripción
Políticas del SGSDP	
Políticas de gestión de datos personales	Deben existir políticas aprobadas por la Alta Dirección 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 relacionadas con el SGSDP deben ser revisadas y evaluadas en su efectividad y cumplimiento periódicamente, así como cuando surja un nuevo riesgo o cambio significativo en la organización.
Documentación del SGSDP	Se deben identificar y documentar de manera proporcional a la organización los activos, políticas, acuerdos, planes estratégicos, procedimientos, controles de seguridad, y todo proceso relacionado al SGSDP.
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, por ejemplo, legislación aplicable a datos de salud.
Salvaguarda de registros organizacionales	Se debe mantener el resguardo de todos los registros y documentación que pudieran ser evidencia o bien, requeridos en cumplimiento de la LFPDPPP y protegerlos contra pérdida, destrucción, falsificación, acceso o revelación no autorizados.

Objetivo de Control	Descripción
Prevención del mal uso de activos	Se deben tener mecanismos contra el uso de activos 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 del SGSDP, 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	La Alta Dirección 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.
Revisión de implementación	Realizar una revisión periódica de la implementación del SGSDP por auditores internos o externos.
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.

Objetivo de Control	Descripción
Requerimientos de seguridad en contratos con terceros	Cuando se establezca un contrato con un tercero, revisar las clausulas 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 computo en la nube, además de revisar las clausulas 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, donde se almacena, como se replica, como 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 los activos	
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.
Inventario de activos	Mantener un registro de los activos de información y de soporte. Identificar a los individuos o grupos de personas dentro o fuera de la organización con responsabilidad sobre los activos.
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.

Objetivo de Control	Descripción
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.
Entrenamiento y educación	Empleados, contrataciones externas y usuarios en general deben recibir concienciación y entrenamiento 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 física	Implementar mecanismos que sólo permitan el acceso 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 a los activos 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 los activos fuera de las instalaciones	Se deben establecer mecanismos autorizados por la Alta Dirección, para controlar la salida fuera de las instalaciones de cualquier activo 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 adecuado. Cualquier eliminación de activos debe registrarse con fines de auditoría.

Objetivo de Control	Descripción
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.
Gestión 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 a 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 los activos.
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 por separación de 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 deberán 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.

Objetivo de Control	Descripción
Políticas del SGSDP	
Políticas de gestión de datos personales	Deben existir políticas aprobadas por la Alta Dirección 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 relacionadas con el SGSDP deben ser revisadas y evaluadas en su efectividad y cumplimiento periódicamente, así como cuando surja un nuevo riesgo o cambio significativo en la organización.
Documentación del SGSDP	Se deben identificar y documentar de manera proporcional a la organización los activos, políticas, acuerdos, planes estratégicos, procedimientos, controles de seguridad, y todo proceso relacionado al SGSDP.
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, por ejemplo, legislación aplicable a datos de salud.
Salvaguarda de registros organizacionales	Se debe mantener el resguardo de todos los registros y documentación que pudieran ser evidencia o bien, requeridos en cumplimiento de la LFPDPPP y protegerlos contra pérdida, destrucción, falsificación, acceso o revelación no autorizados.

4.5.1 Mejores prácticas de seguridad de datos personales.

Las organizaciones deberán establecer de forma anual un comité cccc que tenga como propósito mejorar la seguridad de la información conforme a las necesidades de la organización.

Las prácticas que se recomiendan ejercer son las siguientes:

1. Obligatorias
    a. Selección, implantación y mantenimiento de medidas de seguridad informáticas.
    b. Establecer un departamento de protección de datos personales o su equivalente.
    c. La información confidencial sólo podrá existir en zonas confidenciales.
    d. La información del personal interno, solo podrá existir en la zona de gestión de recursos humanos.
    e. La información privada deberá estar protegida mediante control de accesos.
    f. El propietario de un medio de autenticación es el responsable único del uso de los sistemas o acceso realizados mediante ese medio.
    g. El acceso a servicios confidenciales, personales o financieros no permitirá sesiones simultáneas del mismo usuario.
    h. Las sesiones deben expirar por falta de uso.
    i. Las credenciales expiran por falta de uso.
    j. Deberán adoptarse políticas de contraseñas seguras.
    k. Las zonas donde se maneje información confidencial tendrá una norma sobre el uso de los medio de soporte y tratamiento de la información transportables sean informáticos, físicos o de otro tipo.
    l. Debe evitarse el envío de información confidencial fuera de los sistemas de la organización.
    m. Todo miembro de la organización que trate con datos sensibles debe firmar una declaración de confidencialidad
    n. Preferir el uso de software licenciado.
    o. Existirán métodos de copia de seguridad que garanticen la disponibilidad de la información crítica ante fallos graves del sistema como catástrofes mayores.
    p. Los equipos ´podrán ser identificados como pertenecientes a la organización aunque san robados.
2. Opcionales.
    a. Asistencia a cursos de seguridad de la información y protección de datos personales.
    b. Destrucción diaria del papel
    c. Uso de software cifrado o encriptado.
    d. Controlar el acceso físico a instalaciones.
    e. Se recomienda no utilizar cuentas anónimas.
    f. Uso de antivirus.

   g. Uso de cortafuegos.
3. Prohibidas.
   a. Cesión de medios de autenticación y sesiones de acceso que son personales e intransferibles.
   b. Uso de cualquier material en violación de los derechos de autor por copia fraudulenta o falta de licencia.

4.5.3 Certificaciones de seguridad.

Existen diversas certificaciones para productos específicos de distintos fabricantes, cuanto más es el producto más valiosa es la certificación, las más difundidas son las siguientes:

- GIAC Ofrece varias certificaciones, siendo la más avanzada la de GSE.
- ISC2 ofrece la certificación CISSP
- ISCA ofrece la CISA
- ISEOM ofrece la certificación OPST

El mantener personal con alguno de estos certificados facilita la implementación exitosa de un sistema de seguridad de datos personales en la organización.

4.5.2 Servicios comerciales de seguridad

Distintas empresas ofrecen un gran conjunto de servicios de seguridad, desde el Outsourcing hasta la venta de productos específicos.

Algunos de los servicios especializados que son requeridos para la protección de datos personales son los siguientes:

- Análisis de riesgos
- Comprobación de vulnerabilidades (interna o externa)
- Auditoria
- Consultoría
- Mantenimiento de sistemas (copias de respaldo, cortafuegos)
- Certificación de seguridad de aplicaciones
- Auditoria de código
- Outsourcing de centro de recuperación de desastres
- Formación
- Servicios legales
- Análisis de madurez según el modelo de seguridad

4.5.3 Herramientas para la evaluación de vulnerabilidades.

A continuación se mencionan algunos sitios de internet especializados en seguridad de la información:

- www.microsoft.com/security
- www.linuxsecurity.com
- www.securiteam.com
- www.cert.org
- www.securityfocus.com
- www.parallaxresearch.com
- www.sans.org

Por lo que respecta a detección de virus se encuentran los siguientes servicios en línea:

- http://www.pandasoftware.com/activescan
- http://housecall.antivirus.com

Para verificar la seguridad del navegador o explorar web se encuentran los siguientes servicios:

- http://privacy.net/analyze
- http://www.trustedbase.org/test

A continuación se mencionan dos herramientas para el análisis de puertos abiertos:

- http://scan.sygate.com
- https://grc.com

Mientras que para la prevención de fraudes se encuentran los siguientes sitios web:

- www.rompecadenas.com.ar
- http://hoaxbusters.ciac.org

i