TOOLKIT DE CONCIENTIZACIÓN DE SEGURIDAD DE DATOS PERSONALES PARA RESPONSABLES DEL SECTOR PRIVADO

MÓDULO 4. Medidas de seguridad

Índice

Concepto de medidas de seguridad

La normativa mexicana en materia de protección de datos personales establece que las **medidas de seguridad** son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Asimismo, y al igual que la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares**, se distinguen tres tipos de medidas de seguridad (administrativas, técnicas y físicas) que se explicarán con detalle en los siguientes apartados.

Las medidas de seguridad se pueden agrupar en 10 dominios principales, como se sugiere en la **Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales** que elaboró el INAI.

- Políticas del SGSDP
- Cumplimiento legal
- Estructura organizacional de la seguridad
- Clasificación y acceso de los activos
- Seguridad del personal
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Desarrollo y mantenimiento de sistemas
- Vulneraciones de seguridad

Esta clasificación, responde a los siguientes criterios para elegir las medidas de seguridad efectivas que:

- Protejan los datos personales contra daño, pérdida, destrucción o alteración
- Eviten el uso, acceso o tratamiento no autorizado
- Impidan la divulgación no autorizada de los datos personales

Ahora bien, para determinar qué medidas de seguridad se implementarán para proteger la información y los datos personales, en el **artículo 60 del** **Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares** se sugiere a los responsables que consideren los siguientes factores:

- El riesgo inherente por tipo de dato personal.
- La sensibilidad de los datos personales tratados.
- El desarrollo tecnológico.
- Las posibles consecuencias de una vulneración para personas titulares.
- El número de personas titulares.
- Las vulnerabilidades previas ocurridas en los sistemas de tratamiento.
- 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.
- Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.

En la **Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales** se contempla, en el **Anexo D, una tabla de controles de seguridad** que se puede tomar como referencia para determinar las medidas de seguridad que implementará la institución, sobre todo en función de los factores previamente referidos y de los posibles riesgos que podrían surgir.

En términos generales, el objetivo de las medidas de seguridad de los datos es proteger la información "[…] del acceso no autorizado, la corrupción o el robo durante todo su ciclo de vida. Es un concepto que abarca todos los aspectos de la seguridad de la información, desde la seguridad física del hardware y los dispositivos de almacenamiento hasta los controles administrativos y de acceso, así como la seguridad lógica de las aplicaciones de software. También incluye las políticas y procedimientos de la organización."[1]

De acuerdo con IBM, empresa multinacional de tecnología y consultoría, "cuando se aplican correctamente, las estrategias [(medidas)] de seguridad de datos sólidas protegen los activos de

[1] Disponible en: https://www.ibm.com/topics/data-security

información de una organización contra las actividades de los ciberdelincuentes, pero también protegen contra las amenazas internas y los errores humanos, que siguen siendo una de las principales causas de las vulneraciones de datos hoy en día. La seguridad de los datos implica el despliegue de herramientas y tecnologías que mejoren la visibilidad de la organización sobre dónde residen sus datos críticos y cómo se utilizan. Lo ideal sería que estas herramientas pudieran aplicar protecciones como el cifrado, el enmascaramiento de datos y la redacción de archivos sensibles, y que automatizaran los informes para agilizar las auditorías y el cumplimiento de los requisitos normativos."[2]

[2] Disponible en: https://www.ibm.com/topics/data-security

Medidas de seguridad administrativas

El **Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares**, **específicamente el artículo 2, fracción V**, define las medidas de seguridad administrativas como 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.

Ejemplos:

- Elaborar, aprobar e implementar de una política interna de protección de datos.
- Diseñar, aprobar e implementar de un sistema de gestión de seguridad de datos personales que contemple todos los elementos necesarios.
- Autenticación del personal autorizado para realizar el tratamiento de datos personales.
- Requerir el uso de contraseñas y claves robustas para acceder a los equipos en los que se almacena la información.
- Capacitar al personal en temas relacionados con la seguridad de la información y los datos personales.
- Utilizar conexiones inalámbricas seguras y restringidas.
- Incluir cláusulas de confidencialidad en los contratos laborales.
- Establecer políticas para la clasificación y el almacenamiento de la información.
- Elaborar una política interna sobre el uso de dispositivos móviles fuera de la institución.
- Establecer protocolos para casos de emergencia, sobre todo cuando se detecte una filtración de información.

Medidas de seguridad técnicas

El **Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares**, **específicamente el artículo 2, fracción VII**, se refiere a las medidas de seguridad técnicas como el conjunto de 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.
d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.

Ejemplos:

- Instalar y actualizar de manera periódica antivirus, firewalls y otros programas de seguridad en los equipos electrónicos y de cómputo.
- Utilizar programas autorizados.
- Brindar soporte técnico a los equipos, sistemas y programas.
- Realizar copias de la información en dispositivos de almacenamiento seguro.
- Utilizar técnicas para proteger los datos personales, tales como la encriptación, el cifrado de los datos, la disociación o seudonimización.
- Instalar mecanismos para controlar el acceso del personal a las instalaciones de la institución, especialmente en donde se almacenan los datos personales.
- Monitorear el tratamiento de datos personales.

Medidas de seguridad físicas

El **Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares**, **específicamente el artículo 2, fracción VI**, define las medidas de seguridad físicas como el conjunto de 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, funcionalidad e integridad.
d) Garantizar la eliminación de datos de forma segura.

Ejemplos:

- Proteger las instalaciones, especialmente los espacios en donde se ubican los equipos electrónicos y de cómputo que se utilizan para el tratamiento de datos personales.
- Utilizar mecanismos físicos y/o electrónicos para abrir puertas, cajones, archiveros.
- Instalar sistemas de seguridad que utilicen tecnología de identificación biométrica.
- Garantizar que los equipos electrónicos y de cómputo, así como los documentos físicos, se encuentren debidamente protegidos de factores externos.
- Instalar sistemas de vigilancia, alarmas y demás tecnologías para la prevención de siniestros.

Medidas de seguridad en el cómputo en la nube

El **Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares** se refiere, **en su artículo 52**, al cómputo en la nube, entendido como el modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente.

De acuerdo con el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST, por sus siglas en inglés), el cómputo en la nube es un modelo que permite el acceso ubicuo, conveniente y bajo demanda de red a un conjunto de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que puedan ser rápidamente proveídos con esfuerzos mínimos de administración o interacción con el proveedor de servicios. Este modelo en la nube promueve la disponibilidad y se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de implementación.[3]

La computación en la nube provee entonces numerosas capacidades de almacenamiento y procesamiento de información en centros de datos de terceros; de este modo, cuando un usuario decide utilizar la nube, pierde la habilidad de tener acceso físico a sus datos, y como resultado, confía en que su proveedor de servicios prestará especial atención a la seguridad de su información.

En cuanto a las características esenciales del cómputo en la nube, NIST precisa las siguientes:

- **Autoservicio por demanda:** un consumidor puede abastecerse unilateralmente de capacidades de computación, como tiempo de servidor y almacenamiento en red, según sus

[3] Disponible en: https://transparencia.guadalajara.gob.mx/sites/default/files/DiccionarioProteccionDatosPersonales.pdf

necesidades de forma automática, sin requerir la interacción humana con cada proveedor de servicios.

- **Acceso amplio desde la red:** las capacidades están disponibles sobre la red y se accede a ellas a través de mecanismos estándar que promueven el uso de plataformas heterogéneas tanto pesadas como ligeras (por ejemplo, teléfonos móviles, computadoras portátiles y otros dispositivos).
- **Reservas de recursos en común:** los recursos computacionales del proveedor proponen servir en común a varios usuarios que utilicen un modelo de multiposesión (*multi-tenant model*), con diferentes recursos físicos y virtuales dinámicos y reasignados de acuerdo con la demanda de los consumidores.
- **Rápida elasticidad:** las capacidades pueden suministrarse de manera rápida y elástica (en algunos casos de manera automática) para poder hacer un reajuste de forma. En cuanto al consumidor, las capacidades disponibles para abastecerse a menudo aparecen ilimitadas y se pueden adquirir en cualquier cantidad y en momento.
- **Servicio medido:** los sistemas de nube controlan y optimizan el uso de los recursos de manera automática utilizando una capacidad de medición en un cierto nivel de abstracción adecuado para el tipo de servicio (por ejemplo, almacenamiento, procesamiento, ancho de banda y cuentas de usuario activas). El uso de recursos puede ser monitoreado, controlado y reportado, de esta manera suministra transparencia tanto para el proveedor como para el consumidor del servicio utilizado.[4]

Por otro lado, es importante considerar que existen, al menos tres modelos principales de aprovisionamiento de servicios de cómputo en la nube, a saber:

- **Infraestructura como Servicio (*Infrastructure as a Service* o IaaS):** El Proveedor ofrece acceso directo a almacenamiento, unidades de procesamiento, redes y otros recursos computacionales, para que el cliente utilice a modo el software y/o hardware que requiera. El cliente administra tanto la infraestructura como el software. Por ejemplo: El cliente puede

[4] Disponible en: https://transparencia.guadalajara.gob.mx/sites/default/files/DiccionarioProteccionDatosPersonales.pdf

utilizar, a través de Internet, servicios empresariales tales como: servidores, máquinas virtuales, administración de redes.

- **Plataforma como Servicio (*Platform as a Service* o PaaS):** El proveedor facilita herramientas a sus clientes para que desarrollen sus propias aplicaciones en la plataforma ofrecida. El cliente administra el software, pero no la infraestructura. Por ejemplo: El cliente puede acceder a través de Internet, a plataformas de desarrollo de aplicaciones en línea, para distintos lenguajes de programación, colaborativas y de bases de datos.
- **Software como Servicio (*Software as a Service* o SaaS):** El proveedor suministra programas o aplicaciones que corren completamente en su infraestructura para uso de sus Clientes. El Cliente no tiene control de la infraestructura y sólo tiene control sobre ciertas características del software. Por ejemplo: El cliente puede gestionar correo electrónico, almacenamiento de contenido o mensajería instantánea, a través de software o aplicaciones ofrecidas por el proveedor.[5]

Algunas ventajas de la nube:

- Acceso a la información desde cualquier sitio y a través de diferentes dispositivos.
- Ahorro tanto en software y hardware, como en el mantenimiento técnico.
- Optimizar la asignación y el coste de los recursos asociados a sus necesidades de tratamiento de información.
- Flexibilidad al permitir que no se preste tanta atención a los problemas de almacenamiento de datos.
- Facilidad para recuperar los datos, sobre todo en situaciones de emergencia, tales como catástrofes naturales o incluso cortes de electricidad.
- Se apoya la proactividad ambiental pues se dejan de utilizar productos y hardware físicos, y se reducen los residuos de papel.

Algunas desventajas de la nube:

[5] Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/ComputoEnLaNube.pdf

- Falta de seguridad y privacidad, pues existe la posibilidad de que terceros, especialmente hackers y crackers, accedan de manera ilegal a la información almacenada.
- Dependencia total de Internet, por lo que una falla de conexión imposibilita el acceso a la información almacenada.
- Dificultad para garantizar que el proveedor del servicio cumpla con la normativa correspondiente.
- El usuario, por lo general, tiene un control mínimo del servicio, pues la infraestructura de la nube es propiedad del proveedor de servicios, quien finalmente la gestiona y supervisa.
- Dificultad para migrar la información de un servidor a otro, particularmente cuando el proveedor del servicio no es el mismo.

Ahora bien, debido a que los usuarios de internet pueden utilizar los servicios de cómputo en la nube para almacenar cualquier tiempo de información, incluyendo datos personales y datos personales sensibles, y que existe la posibilidad de que dicha información se vea comprometida por el acceso y la difusión ilegal por parte de hackers y crackers, es esencial que se tomen en cuenta medidas específicas para garantizar su seguridad.

Nos referimos a la seguridad de la nube como una amplia gama de políticas, tecnologías y formas de control, destinadas a proteger los datos, las aplicaciones y la infraestructura asociada a la computación. Su objetivo principal es: almacenar, administrar datos, ejecutar aplicaciones, entregar contenido o servicios. Es decir, la información está disponible con acceso instantáneo donde quiera que se esté y siempre que se necesite a través de la Web.

De hecho, ha comenzado a utilizarse el término "protección de datos en la nube (*cloud data protection*)" para referirse a la práctica de proteger los datos de una empresa en un entorno de nube, dondequiera que se encuentren esos datos, ya sea en reposo o en movimiento, y ya sea gestionado internamente por la empresa o externamente por un tercero.[6] Esto resulta de vital importancia para evitar vulneraciones a la seguridad, pérdida o robo de datos

[6] Disponible en: https://www.paloaltonetworks.com/cyberpedia/what-is-cloud-data-protection

personales y datos personales sensibles, y la exposición de vulnerabilidades de las aplicaciones y la propagación de *malware*.

Es así como han comenzado a surgir diferentes instrumentos jurídicos y de carácter orientador para facilitar a los responsables, tanto del sector público como privado, la implementación de medidas de seguridad.

Por ejemplo, el estándar **ISO 27018 "Requisitos para la protección de la información de identificación personal"** proporciona orientación destinada a garantizar que los proveedores de servicios en la nube puedan ofrecer controles adecuados de seguridad de información con el objetivo de proteger la privacidad de los clientes, o lo que es lo mismo, la seguridad de la información de identificación personal (PII) que se les confía.

Adicionalmente, la norma mexicana **"NMX-I-27018-NYCE-2016-Tecnologías de la información – Técnicas de seguridad – Código de práctica para la protección de datos personales (DP) para proveedores de servicios de nubes públicas"** establece objetivos de control y lineamientos comúnmente aceptados para implementar medidas de protección para los datos personales para ambientes públicos de cómputo en la nube. Es así que se brinda orientación para la implementación de políticas de seguridad de la información; la seguridad en los recursos humanos; la gestión de archivos; el control de acceso; la criptografía; la seguridad física y ambiental; la seguridad en las operaciones; la adquisición, desarrollo y mantenimiento de sistemas, entre otros.

Además, el INAI publicó los **Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales** con el objetivo de establecer consideraciones mínimas que orienten a los responsables del tratamiento de datos personales en la selección y contratación de proveedores, para los servicios de infraestructura, plataforma y software del denominado cómputo en la nube, que ofrezcan garantías de un debido tratamiento de datos personales, a fin de cumplir con las obligaciones que establece la normatividad en la materia y evitar una vulneración en la protección de los datos personales en su posesión.

A continuación, se enlistan algunas medidas de seguridad específicas para la protección de datos durante el uso de la computación en la nube.

Ejemplos:

- Establecer contraseñas.
- Cifrar los datos.
- Limitar y clasificar la información.
- Revisar las configuraciones por defecto.
- Poseer un adecuado sistema de seguridad.

Por otro lado, de conformidad con el artículo 52 del **Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares,** los responsables del tratamiento sólo podrán contratar servicios, aplicaciones e infraestructura en el cómputo en la nube si el proveedor:

- Cumple, al menos, con lo siguiente:
  - Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el presente Reglamento.
  - Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio.
  - Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio.
  - Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.
- Cuenta con mecanismos, al menos, para:
  - Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.
  - Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio.
  - Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio.

- Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos.
- Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

Con el objetivo de facilitar el cumplimiento de lo referido anteriormente, el INAI publicó un documento titulado **"Conformidad de contratos de adhesión de servicios de cómputo en la nube vs los criterios mínimos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales"** que, además de describir los aspectos generales de este modelo, contiene una tabla comparativa para que los responsables del tratamiento de datos personales puedan identificar las condiciones de prestación de servicio de infraestructura, plataforma y software de cómputo en la nube que ofrecen los principales proveedores, y así, elegir y decidir aquellos que más se ajusten a sus necesidades de prestación del servicio de cómputo en la nube.

Estándares

La seguridad de la información se ha convertido en un tema recurrente en la cultura organizacional de empresas e instituciones públicas, sobre todo cuando se toma conciencia del valor de la información y de la importancia de proteger los datos personales para mejorar, por ejemplo, la confianza y la credibilidad institucional o por el simple hecho de evitar una sanción en términos de lo establecido en la legislación y demás normativa de protección de datos personales.

Es por ello por lo que han surgido, a nivel internacional y nacional, diferentes instrumentos orientadores para ayudar a los responsables del tratamiento de datos a proteger la información que utilizan como insumo en sus actividades rutinarias.

A continuación, se enlistan tan solo algunos ejemplos:

- **ISO/IEC 27001. Sistemas de Gestión la Seguridad de la Información:** Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. Este estándar permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.[7]

- **ISO/IEC 27701. Gestión de la privacidad de la información:** Basándose en los requisitos de la ISO/IEC 27001, la ISO/IEC 27701 especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la privacidad de la información (SGPI). Este estándar proporciona el marco del sistema de gestión para proteger la información de identificación personal (IIP). Abarca la forma en que las organizaciones deben gestionar la

[7] Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

información personal y ayuda a demostrar el cumplimiento de las normas de privacidad que puedan aplicarse.[8]

- **Privacy Framework | NIST:** El Marco de Privacidad del Instituto Nacional de Normas y Tecnología (NIST)[9] es una herramienta voluntaria desarrollada en colaboración con las partes interesadas, cuyo objetivo es ayudar a las organizaciones a identificar y gestionar el riesgo de privacidad para crear productos y servicios innovadores, protegiendo al mismo tiempo la privacidad de las personas. Se busca facilitar mejores prácticas de ingeniería de la privacidad compatibles con los conceptos de privacidad desde el diseño y ayudar a las organizaciones a proteger la privacidad de las personas.[10]

- **SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations:** Esta publicación proporciona un catálogo de controles de seguridad y privacidad para que los sistemas de información y las organizaciones protejan las operaciones y los activos de la organización, los individuos, otras organizaciones y la nación de un conjunto diverso de amenazas y riesgos, incluyendo ataques hostiles, errores humanos, desastres naturales, fallos estructurales, entidades de inteligencia extranjeras y riesgos de privacidad. Los controles son flexibles y personalizables y se implementan como parte de un proceso de toda la organización para gestionar el riesgo. Los controles abordan diversos requisitos derivados de las necesidades de la misión y del negocio, leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas y directrices. El catálogo de control consolidado aborda la seguridad y la privacidad desde la perspectiva de la funcionalidad (es decir, la fuerza de las funciones y los mecanismos proporcionados por los controles) y desde la perspectiva de la garantía (es decir, la medida de la confianza en la capacidad de seguridad o privacidad

[8] Disponible en: https://www.dnvgl.es/services/iso-iec-27701-norma-internacional-para-la-gestion-de-la-privacidad-de-la-informacion-159186

[9] El Instituto Nacional de Normas y Tecnología (NIST) fue fundado en 1901 y ahora forma parte del Departamento de Comercio de Estados Unidos. NIST es uno de los laboratorios de ciencias físicas más antiguos del país. Desde la red eléctrica inteligente y las historias clínicas electrónicas hasta los relojes atómicos, los nanomateriales avanzados y los chips informáticos, innumerables productos y servicios dependen de alguna manera de la tecnología, las mediciones y las normas proporcionadas por NIST.

[10] Disponible en: https://www.nist.gov/system/files/documents/2021/01/13/NIST.Privacy.Framework.V1.Spanish.Translation.pdf

proporcionada por los controles). Abordar la funcionalidad y la garantía ayuda a garantizar que los productos de tecnología de la información y los sistemas que se basan en esos productos son suficientemente fiables.[11]

- **Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP):** El objetivo general de este documento es orientar a los responsables y encargados para crear un SGSDP, de manera que a través de un proceso de mejora continua se logre un nivel aceptable del riesgo en el tratamiento de la información personal, de acuerdo con el modelo y objetivos de la organización. El alcance del SGSDP es la protección de los datos personales y su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Es así como el análisis de riesgos y las medidas de seguridad implementadas como resultado del seguimiento de esta guía se deberán enfocar en la protección de datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, así como en evitar las vulneraciones.[12]

- **Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración respecto al riesgo:** Consiste en un documento de apoyo para los responsables (tanto de sector público como del sector privado) con el que pueden identificar las principales amenazas a los datos personales contenidos en los diversos sistemas de tratamiento, así como obtener elementos que les permitan describir, categorizar y ponderar el riesgo respecto de dichas amenazas. Una vez identificadas las amenazas a las que están expuestos los diversos sistemas de tratamiento, los responsables podrán realizar una identificación de las vulnerabilidades en sus sistemas e implementar las medidas de seguridad necesarias (físicas, técnicas o administrativas) o bien adecuar las existentes y con ello reducir la posibilidad de un daño a sus sistemas de tratamiento.[13]

[11] Disponible en: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[12] Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf
[13] Disponible en: https://home.inai.org.mx/wp-content/uploads/AmenazasDP.pdf

- **Recomendaciones para el tratamiento de datos personales y cumplir con el deber de seguridad para instituciones de tecnología financiera (ITF):** En dicho documento se presentan una serie de recomendaciones para proteger los datos personales de los clientes durante diversos procesos que realizan las ITF y que implican el tratamiento de datos, tales como el alta de clientes; la identificación de clientes; la transferencia de datos; el monitoreo de las operaciones; la clasificación de clientes por grado de riesgo; la prevención de lavado de dinero y el financiamiento al terrorismo; la inspección, vigilancia e intercambio de información; la presentación de reportes a la Secretaría de Hacienda y Crédito Público (SHCP) por conducto de la Comisión Nacional Bancaria y de Valores (CNBV); y la conservación de archivos. Asimismo, se enlistan los requerimientos que debe de contemplar el Plan Director de Seguridad de cada ITF para procurar una correcta gestión de la seguridad de la información y evitar que los eventos de seguridad de la información se materialicen en Incidentes de seguridad de la información.[14]

[14] Disponible en: https://home.inai.org.mx/wp-content/uploads/TratamientoDP_FINTECH.pdf

Materiales de difusión

Consulta

Las medidas de seguridad para la protección de los datos personales que se incluyen en la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales del INAI

Artículos de interés

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- ISO 27018 Requisitos para la protección de la información de identificación personal.
- NMX-I-27018-NYCE-2016- Tecnologías de la información – Técnicas de seguridad – Código de práctica para la protección de datos personales (DP) para proveedores de servicios de nubes públicas".
- Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales.
- Conformidad de contratos de adhesión de servicios de cómputo en la nube vs los criterios mínimos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales.
- ISO/IEC 27001. Sistemas de Gestión la Seguridad de la Información.
- ISO/IEC 27701. Gestión de la privacidad de la información.
- Privacy Framework National Institute of Standards and Technology (NIST).
- SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations.
- Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP).
- Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración respecto al riesgo
- Recomendaciones para el tratamiento de datos personales y cumplir con el deber de seguridad para instituciones de tecnología financiera (ITF).

Examen de evaluación

1. **¿Para qué son destinadas las medidas de seguridad físicas según lo establecido en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares?**

a) Para prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información.
b) Para proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones.
c) Para proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad.
d) Para garantizar la eliminación de datos de forma segura
e) Todas las anteriores

2. **¿Qué es el cómputo en la nube de acuerdo con el Instituto Nacional de Estándares y Tecnología de Estados Unidos?**

a) Una metáfora empleada para hacer referencia a servicios que se utilizan a través de Internet.
b) Un modelo que permite el acceso ubicuo, conveniente y bajo demanda de red a un conjunto de recursos informáticos configurables que puedan ser rápidamente proveídos con esfuerzos mínimos de administración o interacción con el proveedor de servicio.
c) Un enfoque popular de servicios de computación como copias de seguridad.
d) Un sistema informático basado en Internet y centros de datos remotos para gestionar servicios de información y aplicaciones.
e) Un conjunto de servicios ofrecidos a través de Internet.

3. **¿Cuáles son los modelos principales de aprovisionamiento de servicios de cómputo en la nube?**

a) Acceso amplio, reservas de uso común y servicio medido de la red
b) Nube pública, privada, híbrida y comunitaria
c) Infraestructura, plataforma y software como servicio
d) Autoservicio de demanda y reservas de uso común
e) Ninguna de las anteriores

4. **De acuerdo con esta característica esencial de cómputo, los sistemas de nube controlan y optimizan el uso de los recursos de manera automática utilizando una capacidad de medición en un cierto nivel de abstracción adecuado para el tipo de servicio.**

a) Rápida elasticidad
b) Acceso amplio desde la red
c) Reservas de recursos en común
d) Servicio medido
e) Autoservicio por demanda

5. **Gracias a ello, la información está disponible con acceso instantáneo donde quiera que se esté y siempre que se necesite a través de la Web.**

a) Protección de datos en la nube
b) Seguridad en la nube
c) Privacidad de datos en la nube
d) Almacenamiento de la nube
e) Todas las anteriores

6. **Es el estándar internacional de privacidad en la nube que proporciona orientación destinada a garantizar que los proveedores de servicios en la nube puedan ofrecer controles adecuados de seguridad de información con el objetivo de proteger la privacidad de los clientes**

a) ISO 27001

b) ISO 27000
c) ISO 27017
d) ISO 27701
e) ISO 27018

7. Establece objetivos de control y lineamientos comúnmente aceptados para implementar medidas de protección para los datos personales para ambientes públicos de cómputo en la nube.

a) Norma mexicana NMX-I-27018-NYCE-2016
b) Cloud data protection
c) Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los particulares
d) Lineamientos generales de protección de datos personales en posesión de sujetos obligados
e) Ninguna de las anteriores

8. Es un ejemplo de medida de seguridad específica para la protección de datos durante el uso de la computación en la nube.

a) Establecer Contraseñas y cifrar datos
b) Limitar y clasificar la información
c) Revisar las configuraciones por defecto
d) Poseer un adecuado sistema de seguridad
e) Todas las anteriores

9. El INAI publicó este documento con el objetivo de identificar las condiciones de prestación de servicio de infraestructura, plataforma y software de cómputo en la nube que ofrecen algunos proveedores y, de esta manera, ayudar a los responsables a elegir y decidir aquellos que más se ajusten a sus necesidades de prestación del servicio de cómputo en la nube.

a) Conformidad de contratos de adhesión de servicios de cómputo en la nube vs los criterios mínimos para la contratación de

servicios de cómputo en la nube que impliquen el tratamiento de datos personales

b) Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales
c) Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales
d) Guía para instrumentar medidas compensatorias en el sector público
e) Ninguna de las anteriores

10. ¿Cómo se denomina a las personas que violan la seguridad y privacidad de los datos personales en la nube?

a) Cibernéticos
b) Informáticos
c) Hackers y crackers
d) Violadores de nube
e) Programadores