Cartillas Cámara

4/2023

SL LEGAL + TECNOLOGÍA

CAMARA DE COMERCIO®
DE MEDELLIN PARA ANTIOQUIA



Guía de buenas prácticas en protección de datos personales y ciberseguridad

El contenido de esta cartilla fue elaborado por la Cámara de Comercio de Medellín para Antioquia y SL Legal + Tecnología.

Mayo de 2023.

Autor:
Andrés Felipe Ángel
Director SL Legal + Tecnología

Cámara de Comercio de Medellín para Antioquia:
Lina Vélez de Nicholls
Presidenta Ejecutiva

Jorge Villegas Betancur
Secretario General y Vicepresidente de Asuntos Legales y Corporativos

Equipo técnico:
Liliana María Castillo Restrepo
Directora Jurídica

Natalia Isaza Jaramillo
Jefe de Estudios Jurídicos

Santiago Ramírez Builes
Abogado de Estudios Jurídicos

Coordinación editorial:
Vicepresidencia de Proyección Corporativa y Entorno

Edición y diagramación:
Marcela Hernández Sansón y Andrea Lopera / Blanco Contenido

Todos los derechos reservados
Cámara de Comercio de Medellín para Antioquia
Calle 53 # 45-77, Medellín

CONTENIDO

1. Introducción 4
2. Fundamentos de la protección de datos personales y la ciberseguridad 5
3. Normas y estándares para la protección de datos personales 8
4. Implementación de controles de ciberseguridad y de privacidad de los datos 14
5. Monitoreo y mejora continua 17
6. Casos prácticos 20

1. Introducción

La protección de los datos personales y la ciberseguridad son temas relevantes en el mundo digital, donde la información personal se ha convertido en un recurso valioso tanto para las empresas como para los cibercriminales, lo que ha incrementado la necesidad de salvaguardarla y garantizar la privacidad de los usuarios.

A esto se suma el crecimiento exponencial de las redes sociales y de las plataformas en línea, donde hay un intercambio constante de información personal que puede ser robada y usada con fines maliciosos, como la suplantación de identidad, el fraude, el ciberacoso, la pornovenganza, entre otros. Bajo ese contexto, la ciberseguridad se vuelve fundamental para proteger a los individuos y a las organizaciones de estas amenazas, así como para mantener la confianza en el ecosistema digital.

A su vez, el cumplimiento de las legislaciones y regulaciones en materia de protección de los datos y la privacidad, como la Ley 1581 de 2012 de Protección de Datos Personales (LEPDP) y el Reglamento General de Protección de Datos (RGPD) en Europa, es esencial para evitar sanciones y garantizar el respeto de los derechos de los ciudadanos relacionados con su información.

Esta guía proporciona una descripción general de las legislaciones y regulaciones relevantes, de la ciberseguridad y de las obligaciones de los responsables y encargados del tratamiento de datos, además de entregar casos prácticos reales que ilustran cómo aplicar estos conceptos en situaciones cotidianas.

2. Fundamentos de la protección de datos personales y la ciberseguridad

2.1. CONCEPTOS BÁSICOS DE LA PROTECCIÓN DE DATOS PERSONALES

▸ **Datos personales:** es la información relacionada con una persona natural identificada o identificable. Esto incluye, por ejemplo, nombre, dirección, teléfono, correo electrónico y número de identificación.

▸ **Tratamiento:** cualquier operación o conjunto de operaciones que se realicen con los datos personales, como su recopilación, almacenamiento, modificación, uso, divulgación o eliminación.

▸ **Responsable del tratamiento:** persona natural o jurídica, autoridad pública, servicio u organismo que, solo o junto con otros, determina los fines y medios del tratamiento de los datos personales.

▸ **Encargado del tratamiento:** persona natural o jurídica, autoridad pública, servicio u organismo que trata datos personales en nombre del responsable del tratamiento.

▸ **Principios de la protección de datos:** reglas esenciales sobre el tratamiento de los datos personales relacionadas con su captura, administración y divulgación.

2.2. CONCEPTOS BÁSICOS DE CIBERSEGURIDAD

▸ **Ciberseguridad:** acciones destinadas a proteger los sistemas, las redes y los programas informáticos de ataques digitales, daños o accesos no autorizados.

▸ **Amenaza:** Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad. (Ministerio de Asuntos Económicos y Transformación Digital e Instituto Nacional de Ciberseguridad [Incibe], 2020, p. 14)

▸ **Vulnerabilidades:** «Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina *exploit*). Cuando se descubre el desarrollador del *software* o *hardware* lo solucionará publicando una actualización de seguridad del producto" (Ministerio de Asuntos Económicos y Transformación Digital e Incibe, 2020, p. 77).

▸ **Medidas de seguridad:** acciones, tecnologías y prácticas implementadas para proteger sistemas, redes y datos de amenazas cibernéticas y garantizar la confidencialidad, integridad y disponibilidad de la información.

▸ **Gestión de riesgos de ciberseguridad:** proceso de identificar, evaluar y abordar riesgos de ciberseguridad, incluyendo la implementación de medidas de prevención, detección, respuesta y recuperación.

2.3. RELACIÓN ENTRE LA PROTECCIÓN DE DATOS PERSONALES Y LA CIBERSEGURIDAD

La protección de los datos personales y la ciberseguridad están estrechamente relacionadas porque la segunda es crucial

para garantizar la privacidad y protección de los datos personales. Las organizaciones que tratan estos datos deben implementar medidas de seguridad adecuadas para protegerlos de amenazas cibernéticas y cumplir con las leyes y regulaciones que les son aplicables.

Los incidentes de ciberseguridad, como los incidentes en la seguridad de los datos personales, pueden generar graves consecuencias para los individuos cuyos datos se ven afectados y para las organizaciones responsables de su tratamiento. Entre las posibles repercusiones están el deterioro de la reputación, pérdidas económicas, multas y sanciones legales, así como la disminución de la confianza por parte de clientes y usuarios.

Para mitigar estos riesgos es fundamental que las organizaciones adopten un enfoque proactivo. Por ejemplo, capacitar al personal, implementar políticas y procedimientos claros y efectivos y establecer mecanismos de monitoreo y respuesta de incidentes. De esta manera se fortalece la protección de los datos personales y se promueve un entorno digital seguro y confiable para los involucrados.



3. Normas y estándares para la protección de datos personales

Cada país y región puede tener sus propias leyes y reglamentaciones en protección de datos personales. Por lo tanto, es fundamental que las organizaciones conozcan las legislaciones que aplican en los lugares donde operan. En esta guía tendremos en cuenta las siguientes normas y estándares:

3.1. LEY 1581 DE 2012 DE COLOMBIA

- Establece las disposiciones generales para la protección de datos personales de los ciudadanos colombianos.

- **Ámbito de aplicación:** se aplica a organizaciones públicas y privadas que traten datos personales en Colombia o de ciudadanos colombianos fuera del país.

- **Principios rectores:** establece principios rectores para el tratamiento de datos personales, como la legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

- **Autorización:** exige que las organizaciones obtengan la autorización expresa e informada de los titulares antes de tratar sus datos personales, a menos que exista una excepción legal aplicable.

- **Derechos de los titulares:** les otorga a los titulares de los datos personales varios derechos, como el acceso, consulta, rectificación, actualización, supresión y revocación de la autorización. Igualmente, pueden presentar quejas ante la autoridad de protección de datos.

▸ **Responsabilidad y gobernanza:** exige a las organizaciones implementar políticas y prácticas adecuadas para garantizar el cumplimiento de sus disposiciones y proteger los datos personales de los titulares de accesos no autorizados y de incidentes de seguridad.

3.2. RGPD DE LA UNIÓN EUROPEA (UE)

▸ Establece normas para la protección de los datos personales de los ciudadanos de la UE y del Espacio Económico Europeo (EEE). Sus principales objetivos son garantizar la privacidad y la protección de los datos personales de los individuos y armonizar las leyes de protección de datos en toda la UE.

▸ **Ámbito de aplicación:** se aplica a organizaciones establecidas en la UE y el EEE y a aquellas que están fuera de estos territorios, pero que tratan datos personales de individuos en la UE y el EEE en relación con la oferta de bienes y servicios o el monitoreo de su comportamiento.

▸ **Principios:** establece ocho principios que rigen el tratamiento de los datos personales: licitud, lealtad, transparencia, limitación de la finalidad, minimización de los datos, exactitud, limitación del almacenamiento y la integridad y confidencialidad.

▸ **Consentimiento:** exige que las organizaciones obtengan el consentimiento explícito e informado de los individuos antes de tratar sus datos personales, a menos que exista otra base legal para el tratamiento.

▸ **Derechos de los individuos:** les otorga a los individuos varios derechos en relación con sus datos personales,

como el acceso, rectificación, supresión (derecho al olvido), oposición, limitación del tratamiento y portabilidad de los datos.

▸ **Responsabilidad y gobernanza:** introduce el concepto de «responsabilidad proactiva» que les exige a las organizaciones demostrar que cumplen con las disposiciones del RGDP implementando políticas, procesos y tecnologías adecuadas.

3.3. NORMA ISO/IEC 27701 GESTIÓN DE LA PRIVACIDAD DE LA INFORMACIÓN

▸ Es una norma internacional que proporciona un marco para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de la Privacidad de la Información (SGPI).

▸ Esta norma es una extensión de la popular ISO/IEC 27001, que se centra en la gestión de la seguridad de la información.



▸ Se publicó en agosto de 2019 y tiene como objetivo ayudar a las organizaciones a proteger los datos personales y a cumplir con las regulaciones de privacidad y protección de datos, como el RGPD en la UE.

▸ **Estructura del marco**: tiene ocho secciones principales y seis anexos. Establece requisitos adicionales y pautas de implementación que se integran al marco normativo de las normas ISO 27001 e ISO 27002 para facilitar la adopción del SGPI.

▸ Asimismo, la norma ISO 27701 proporciona un mapeo entre esta y otras normas relevantes como la ISO 29100, ISO 27018 e ISO 29151. También incluye una relación entre sus principios y los requerimientos del RGPD.

▸ **Enfoque basado en riesgos:** al utilizar un enfoque centrado en riesgos, la ISO/IEC 27701 les proporciona a las empresas las herramientas para abordar de manera efectiva los riesgos particulares de privacidad y aquellos asociados a los datos personales y la privacidad de sus clientes. Este enfoque facilita el tener una gestión eficiente y ajustada a los requerimientos de cada organización.

▸ **Flexibilidad y adaptabilidad:** está diseñada para adaptarse a las necesidades, contextos y requisitos legales y normativos de cada organización, independientemente de su tamaño, sector o ubicación geográfica. Esta flexibilidad les permite a las organizaciones implementar un SGPI ajustado a sus propias circunstancias y riesgos, en lugar de seguir un conjunto de reglas rígido y preestablecido.

▸ **Extensión de la ISO/IEC 27701:** es una extensión de la ISO 27001 en materia de privacidad y se integra con esta norma y con la ISO 27002, lo que facilita incorporar los requisitos de privacidad en el sistema de gestión de la seguridad de la información (SGSI) de la organización. De esta manera las empresas pueden aprovechar los procesos y controles de seguridad de la información ya implementados y adaptarlos para abordar también las preocupaciones de privacidad.

3.4. MARCO DE PRIVACIDAD NIST

▸ Es un conjunto de prácticas, directrices y herramientas desarrolladas por el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) de los Estados Unidos para ayudar a las organizaciones a gestionar y proteger la privacidad de los datos personales y cumplir con las regulaciones y estándares aplicables.

▸ **Estructura del marco:** se basa en cinco funciones principales: identificar, gobernar, controlar, comunicar y proteger. Cada función se divide en categorías y subcategorías que describen prácticas y actividades específicas relacionadas con la gestión de la privacidad de los datos personales.

▸ **Enfoque basado en riesgos:** adopta un enfoque basado en riesgos para la gestión de la privacidad de los datos personales. Esto les facilita a las organizaciones identificar y abordar de manera efectiva los riesgos de privacidad asociados con el tratamiento de los datos personales.

▸ **Flexibilidad y adaptabilidad:** es flexible y adaptable, por lo que las organizaciones pueden ajustar sus prácticas de privacidad de datos personales en función de sus necesidades específicas, el contexto y los requisitos legales y normativos aplicables.

▸ **Integración con el Marco de Ciberseguridad NIST:** el Marco de Privacidad NIST se puede integrar con el Marco de Ciberseguridad NIST, lo que les permite a las organizaciones gestionar de manera holística tanto la privacidad como la ciberseguridad de los datos personales.



4. Implementación de controles de ciberseguridad y de privacidad de los datos

En esta sección se aborda la implementación de controles de ciberseguridad y de privacidad de los datos en una organización. Estos pasos pueden ayudar a la organización a tener un enfoque sólido y holístico para proteger los datos personales y cumplir con las leyes, regulaciones y estándares aplicables.

Ten en cuenta que los controles que se mencionan no son exhaustivos y, por su naturaleza, son dinámicos, ya que dependen directamente del avance tecnológico. Por lo tanto, estas medidas están sujetas a constantes actualizaciones.

4.1. EVALUACIÓN DE RIESGOS Y BRECHAS

- **Realizar evaluaciones de riesgos periódicas:** identificar y evaluar los riesgos de ciberseguridad y privacidad en relación con el tratamiento de los datos personales y los sistemas de información utilizados.

- **Identificar brechas de cumplimiento:** evaluar las prácticas actuales de la organización relacionadas con las regulaciones y estándares aplicables (Ley 1581 de 2012, RGPD, Marco de Privacidad NIST y Normas ISO/IEC 27701) para identificar brechas y áreas de mejora.

4.2. IMPLEMENTACIÓN DE POLÍTICAS Y PROCEDIMIENTOS

- **Política de privacidad y ciberseguridad:** establecer políticas y procedimientos escritos que estipulen cómo la organización protegerá la privacidad de los datos personales y garantizará la ciberseguridad.

▸ **Procedimientos de respuesta a incidentes:** desarrollar e implementar procedimientos para detectar, responder y recuperarse de incidentes de seguridad e incidentes de seguridad de datos personales.

▸ **Programas de capacitación y concientización:** implementar programas de capacitación y concientización en ciberseguridad y privacidad dirigidos a empleados y al personal clave. Estas capacitaciones deben evaluarse para obtener información sobre la comprensión de los temas tratados así como indicadores para el programa de protección de datos.

4.3. CONTROLES TÉCNICOS

▸ **Encriptación:** utilizar encriptación para proteger los datos personales en reposo (información almacenada en dispositivos físicos o sistemas, como discos duros, servidores, bases de datos, dispositivos móviles o copias de seguridad) y los datos en tránsito (información que se transmite a través de redes, sean públicas o privadas, como internet e intranet).

▸ **Control de acceso:** instaurar controles basados en roles para permitir el acceso a los sistemas y a los datos personales solo a aquellos empleados que lo necesiten para realizar sus laborales.

▸ **Monitoreo y detección de amenazas:** implementar sistemas de monitoreo y detección de amenazas para identificar y responder rápidamente a los incidentes de seguridad y a los incidentes de seguridad de datos personales.

▸ **Copias de seguridad y recuperación de datos:** establecer procesos para realizar copias de seguridad de los datos personales y garantizar su recuperación en caso de pérdida, corrupción o destrucción.

4.4. CONTROLES ORGANIZATIVOS

▸ **Designar un responsable de la protección de los datos (DPO)** para supervisar y gestionar el cumplimiento de las regulaciones y de los estándares de ciberseguridad y de la privacidad de los datos dentro de la organización.

▸ **Evaluar el impacto de privacidad (PIA)** para identificar y minimizar los riesgos de privacidad asociados con el tratamiento de los datos personales en proyectos y actividades específicas.

▸ **Gestionar a proveedores y terceros:** establecer políticas y procedimientos para evaluar y gestionar los riesgos de privacidad y ciberseguridad asociados con proveedores y con terceros que tratan datos personales en nombre de la organización.

▸ **Realizar auditorías y revisiones periódicas** para evaluar la efectividad de los controles de ciberseguridad y privacidad implementados y asegurar el cumplimiento continuo de las regulaciones y de los estándares aplicables.

5. Monitoreo y mejora continua

5.1. SEGUIMIENTO Y MONITOREO DEL PROGRAMA

▸ **Establecer indicadores claves de rendimiento (KPI)** para monitorear la efectividad y el rendimiento del programa de ciberseguridad y privacidad de los datos.

▸ **Monitoreo y reporte regular:** monitorear los KPI periódicamente y generar informes para la dirección y las partes interesadas sobre el progreso y los resultados del programa de ciberseguridad y privacidad.

▸ **Retroalimentación y comunicación:** facilitar la comunicación abierta y transparente entre los empleados, la dirección y las partes interesadas sobre el programa de ciberseguridad y privacidad y sobre cualquier preocupación o problema relacionado.

5.2. REVISIONES Y AUDITORÍAS

▸ **Revisiones internas:** hacer revisiones internas periódicas del programa de ciberseguridad y privacidad de datos para evaluar su efectividad y garantizar el cumplimiento continuo de las regulaciones y de los estándares aplicables.

▸ **Auditorías externas:** contratar a auditores externos, si corresponde, para realizar auditorías independientes del programa de ciberseguridad y privacidad de datos y hacer recomendaciones de mejora.

▸ **Seguimiento de acciones correctivas:** rastrear y monitorear la implementación de acciones correctivas y de las mejoras identificadas en las revisiones y las auditorías internas y externas.

5.3. AJUSTES Y MEJORAS DEL PROGRAMA

▸ **Análisis de lecciones aprendidas:** revisar y analizar las lecciones aprendidas de los incidentes de seguridad y los incidentes de seguridad de datos personales, de las auditorías y de las revisiones para identificar las mejoras necesarias en el programa de ciberseguridad y privacidad de datos.

▸ **Actualización de políticas y procedimientos de ciberseguridad y privacidad de datos:** revisarlos y actualizarlos periódicamente para incorporar los cambios en las regulaciones, estándares, tecnologías y prácticas de la industria.

▸ **Evaluar las capacitaciones y las acciones de concienciación:** evaluar y mejorar continuamente el programa de capacitación y concienciación en ciberseguridad y privacidad de datos para garantizar que los empleados estén informados y preparados para responder a las últimas amenazas.

5.4. ADAPTACIÓN A LOS CAMBIOS REGULATORIOS Y DEL ENTORNO

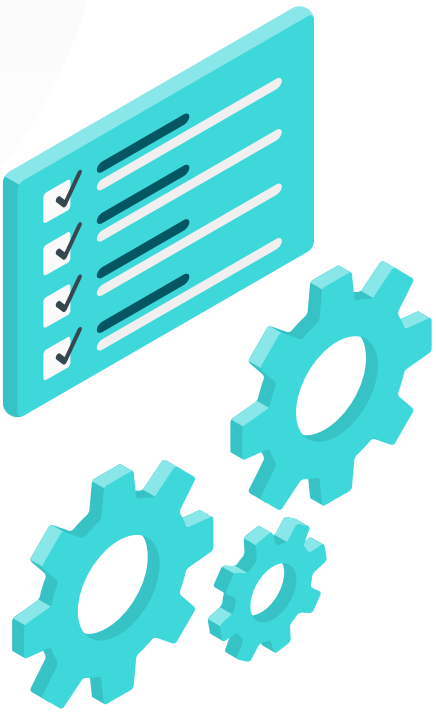
▸ **Monitoreo de cambios regulatorios:** mantenerse informado sobre los cambios en las regulaciones y en los estándares de la protección de datos personales y la ciberseguridad, como la Ley 1581 de 2012, el RGPD, el Marco de

Privacidad NIST, los pronunciamientos de las autoridades de protección de datos, entre otros.

- **Evaluación del impacto de los cambios regulatorios:** evaluar el impacto que los cambios regulatorios tienen en la organización y, en consecuencia, adaptar el programa de ciberseguridad y privacidad de datos.

- **Ajuste a las nuevas tecnologías y tendencias:** actualizarse en las últimas tecnologías y tendencias en ciberseguridad y privacidad de datos e incorporarlas en el programa, según corresponda.

Aunque el listado no es exhaustivo, al seguir estos pasos las organizaciones pueden asegurarse de que su programa se mantenga actualizado y sea efectivo en un entorno en constante cambio y evolución.



6. Casos prácticos

Los siguientes casos sirven para comprender cómo las organizaciones aplican la protección de los datos personales y las prácticas de ciberseguridad en diferentes situaciones. También permiten identificar cómo enfrentarse a situaciones reales y aplicar las estrategias presentadas anteriormente.

En estos ejemplos se destaca la importancia de la evaluación continua, de la mejora de las estrategias, de las medidas de seguridad y del cumplimiento de las leyes y las regulaciones aplicables.

6.1. CASO PRÁCTICO 1. INCIDENTES DE SEGURIDAD DE DATOS PERSONALES Y SU GESTIÓN

Una empresa de comercio electrónico experimentó una violación de datos. Personas ajenas a la organización accedieron a bases de datos y filtraron los datos personales de 50.000 clientes, incluidos nombres, direcciones, teléfonos y detalles de las tarjetas de crédito. La empresa siguió un enfoque de respuesta a incidentes que incluyó:

- **Detección y análisis del incidente:** detectó la violación a través de su sistema de monitoreo de seguridad y analizó su naturaleza y alcance.

- **Contención y erradicación:** tomó medidas inmediatas para contener la violación, aislar los sistemas afectados y eliminar el acceso no autorizado.

- **Recuperación y restauración:** restauró sus sistemas a un estado seguro y recuperó los servicios afectados.

▸ **Notificación a las autoridades y a las partes afectadas:** se informó a las autoridades de protección de datos y a los clientes afectados, según lo exigido por la legislación aplicable.

En Colombia, los incidentes de seguridad de datos personales deben reportarse a las autoridades correspondientes dentro los quince días hábiles siguientes al momento en que se detectan y son puestos en conocimiento de la persona o del área encargada de atenderlos.

Por su parte, el RGPD establece que el responsable del tratamiento notificará las brechas de datos personales a la autoridad de control sin dilación indebida y, a más tardar, dentro de las 72 horas (incluyendo fines de semana y festivos) siguientes al momento en el que el responsable del tratamiento tenga constancia de que el incidente de seguridad afectó los datos personales (Agencia Española de Protección de Datos [AEPD], 2021, p. 18).

▸ **Análisis de lecciones aprendidas y mejora del programa de seguridad:** la empresa revisó la violación de datos y las acciones tomadas, identificó áreas de mejora y ajustó su programa de ciberseguridad y privacidad de datos.

6.2. CASO PRÁCTICO 2. EVALUACIÓN DE IMPACTO EN LA PRIVACIDAD (PIA, POR SUS SIGLAS EN INGLÉS)

Una organización de atención médica planeó implementar un nuevo sistema de registros médicos electrónicos que involucraba el procesamiento de datos personales sensibles. La organización llevó a cabo una PIA siguiendo estos pasos:

▸ **Identificación de la necesidad de la PIA:** se determinó que el proyecto requería una PIA debido a la naturaleza

sensible de los datos personales involucrados y al potencial riesgo alto para los derechos y libertades de los individuos.

- **Descripción del proyecto y evaluación de riesgos:** la organización describió el proyecto en detalle, identificó los riesgos asociados con el procesamiento de los datos personales y evaluó la probabilidad y el impacto de cada uno.

- **Identificación y aplicación de medidas de mitigación:** la organización identificó y aplicó medidas de mitigación de riesgos, como la encriptación de datos, la implementación de controles de acceso y la capacitación del personal en privacidad y seguridad de los datos.

- **Consulta con las partes interesadas y revisión de la PIA:** consultaron a las partes interesadas relevantes (incluidos los empleados, los pacientes y las autoridades de protección de datos) para conocer sus opiniones y asegurar la solidez de la PIA. Luego la revisaron y ajustaron.

- **Monitoreo y revisión periódica:** se estableció un proceso de monitoreo y revisión periódica de la PIA para garantizar que las medidas de mitigación de riesgos sean efectivas y capaces de adaptarse a los cambios en un entorno de riesgo.

6.3. CASO PRÁCTICO 3. CAPACITACIÓN Y CONCIENTIZACIÓN EN CIBERSEGURIDAD Y EN PRIVACIDAD DE LOS DATOS

Una empresa de servicios financieros implementó un programa de capacitación y concientización para sus empleados sobre ciberseguridad y privacidad de los datos que incluyó:

- **Identificación de necesidades de capacitación:** evaluaron las necesidades de capacitación y concienciación de sus empleados en función de sus roles y responsabilidades en relación con el procesamiento de datos personales y la seguridad de la información.

- **Desarrollo e implementación del programa:** el programa abordaba temas clave como el cumplimiento normativo, las políticas y procedimientos de la empresa y las mejores prácticas de seguridad.

- **Evaluación de la efectividad:** se evaluó el programa mediante pruebas, encuestas y el seguimiento de los incidentes relacionados con la seguridad y la privacidad de los datos.

- **Mejora continua:** la empresa usó los resultados de la evaluación para mejorar y actualizar el programa de capacitación y concienciación, asegurando que se mantuviera relevante y efectivo en un entorno de riesgo en constante evolución.

6.4. CASO PRÁCTICO 4. GESTIÓN DE TERCEROS Y RIESGOS EN LA CADENA DE SUMINISTRO

Una empresa de tecnología que subcontrataba con terceros el desarrollo de *software* y el alojamiento en la nube implementó un proceso de gestión de riesgos en la cadena de suministro que incluyó:

- **Evaluación de riesgos de terceros:** evaluaron los riesgos asociados con los proveedores y con terceros en función de la naturaleza de los servicios prestados y de los datos personales a los que tenían acceso.

- **Establecimiento de requisitos contractuales:** en los contratos con proveedores y con terceros se incluyeron disposiciones específicas sobre la seguridad de la información, la privacidad de los datos y la responsabilidad en caso de su incumplimiento.

- **Monitoreo y auditoría:** se estableció un proceso de monitoreo y auditoría para garantizar que proveedores y terceros cumplieran con sus obligaciones contractuales y legales en materia de seguridad de la información y privacidad de los datos.

- **Mejora y revisión:** la empresa revisó regularmente su enfoque de gestión de riesgos en la cadena de suministro y ajustó sus prácticas y requisitos contractuales según fuera necesario para abordar los cambios en el entorno de riesgo y garantizar un nivel adecuado en la protección de los datos y la ciberseguridad.

6.5. CASO PRÁCTICO 5. IMPLEMENTACIÓN DE POLÍTICAS Y PROCEDIMIENTOS DE PROTECCIÓN DE LOS DATOS PERSONALES Y DE CIBERSEGURIDAD

Una empresa de comercio electrónico estableció políticas y procedimientos de privacidad y ciberseguridad para garantizar el cumplimiento normativo y proteger los datos personales de sus clientes. El proceso incluyó:

- **Desarrollo de políticas y procedimientos:** se desarrollaron políticas y procedimientos que abordaban aspectos clave como la recolección y procesamiento de datos personales, los derechos de los titulares de datos, la seguridad de la información y la respuesta a incidentes.

- **Comunicación y capacitación:** la empresa comunicó sus políticas y procedimientos a los empleados y los capacitó sobre cómo implementarlos en sus roles y responsabilidades diarias.

- **Monitoreo y aplicación:** se establecieron mecanismos de monitoreo y aplicación para garantizar el cumplimiento de sus políticas y procedimientos y abordar cualquier incumplimiento o desviación.

- **Revisión y actualización periódica:** realizaron revisiones y actualizaciones periódicas de sus políticas y procedimientos para garantizar que se mantuvieran al día con los cambios en la legislación, las expectativas de los clientes y las amenazas y riesgos de ciberseguridad.

6.6. CASO PRÁCTICO 6. IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD ADECUADAS

Una organización sin fines de lucro que maneja datos personales sensibles de sus beneficiarios identificó y aplicó medidas de seguridad adecuadas para proteger los datos almacenados y procesados en sus sistemas. Algunas de las medidas implementadas fueron:

- **Encriptación de datos en reposo y en tránsito:** encriptaron los datos para proteger la información sensible tanto en reposo como en tránsito.

- **Autenticación multifactor:** se implementó la autenticación multifactor para garantizar que solo los autorizados pudieran acceder a los sistemas y a los datos.

▸ **Seguridad de red y monitoreo:** se establecieron *firewalls*, sistemas de detección de intrusiones y herramientas de monitoreo para proteger la infraestructura de red y detectar posibles amenazas.

▸ **Capacitación y concienciación de seguridad:** periódicamente se capacitó al personal en prácticas de seguridad, como la identificación de estafas de *phishing* y la importancia de mantener actualizados los *software* y sistemas.

Caja de herramientas

Comissão Nacional de Proteção de Dados (2023). *DIRETRIZ/2023/1 Sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais*. https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/122048

-

Posada Ángel, F. A. (2021). Checklist *para evitar incidentes de seguridad de datos en las empresas*. Cámara de Comercio de Medellín para Antioquia y Tecnología + Legal SL. https://www.camaramedellin.com.co/biblioteca/checklist-para-evitar-incidentes-de-seguridad-de-datos-en-las-empresas

-

Posada Ángel, F. A. (2022). *Guía para la función del oficial de protección de datos personales*. Cámara de Comercio de Medellín para Antioquia y Tecnología + Legal SL. https://www.camaramedellin.com.co/biblioteca/guia-para-la-funcion-del-oficial-de-proteccion-de-datos-personales-1

-

Red Iberoamericana de Protección de Datos. (2017). *Estándares de protección de datos personales*. https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

-

Red Iberoamericana de Protección de Datos. (2022). *Guía de implementación de cláusulas contractuales modelo para la transferencia internacional de datos personales (TIDP)*. https://www.redipd.org/sites/default/files/2022-09/guia-clausulas-contractuales-modelo-para-tidp.pdf

-

Stand der Technik. (2023). Datenschutzstelle Fürstentum Liechtenstein. https://www.datenschutzstelle.li/aktuelles/stand-der-technik

Referencias

► Agencia Española de Protección de Datos. (2021). *Guía para la notificación de brechas de datos personales*. https://www.aepd.es/es/documento/guia-brechas-seguridad.pdf

► Ministerio de Asuntos Económicos y Transformación Digital e Instituto Nacional de Ciberseguridad. (2020). *Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario*. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

CAMARA DE COMERCIO®
DE MEDELLIN PARA ANTIOQUIA

Tu mejor socio.

ENCUÉNTRANOS

@camaramedellin | camaramedellin | CamaraMedellin | Cámara de Comercio de Medellín | Cámara de Comercio de Medellín

ESCÚCHANOS

cámarafm95.9®

camaramedellin.com