Gestión de riesgos, continuidad y terceros

CÓRDOBA CREA FUTURO

La gestión de riesgos, la continuidad del negocio y la gestión de terceros son grandes pilares en la seguridad de la información.

Este módulo aborda cómo identificar y valorar riesgos de información, cómo asegurar la continuidad operativa ante crisis y cómo controlar los riesgos asociados a proveedores y terceros externos.

Unidad 1: Riesgo y elementos de la gestión de continuidad y recuperación ante desastres (BIA/BCP/DRP

Unidad 1: Riesgo y elementos de la gestión de continuidad y recuperación ante desastres (BIA/BCP/DRP)

1. 1. BIA (*business impact analysis* o análisis del impacto en el negocio)

En esta sección, se hará una introducción sobre los conceptos de gestión de riesgos, antes de introducir el concepto de BIA. Mencionamos ahora los conceptos de procesos críticos y métricas usadas en la gestión de riesgos, tales como MTPD (tiempo máximo de caída tolerable), RTO (tiempo de recuperación objetivo) y RPO (punto de recuperación objetivo). En secciones posteriores, se ampliarán estas definiciones y su aplicación.

Gestión de riesgos

En seguridad de la información, la gestión de riesgos es el proceso sistemático de identificar, evaluar y tratar los riesgos asociados al uso de tecnologías y activos de información. Su objetivo es proteger los activos organizacionales y garantizar el cumplimiento de los objetivos empresariales.

La gestión de riesgos está orientada a la toma de decisiones basada en información precisa. Por ejemplo, un riesgo alto justifica más controles; uno bajo puede asumirse. Además, es clave el contexto de negocio: un riesgo que para una empresa es crítico puede ser tolerable en otra con distinto apetito de riesgo. La documentación resultante suele plasmarse en un **registro de riesgos** o matriz de riesgos, que incluye la descripción del riesgo, causa, impacto, nivel de riesgo y acciones de tratamiento.

La gestión de riesgos es un enfoque estructurado para manejar la incertidumbre ante amenazas. Para ello, se sigue un ciclo continuo de gestión de riesgos que, según la norma ISO 31000 (International Organization for Standardization [ISO], 2018), típicamente, incluye lo siguiente:

- **establecer el contexto**. Definir objetivos, alcance y criterios de riesgo según el entorno

interno (procesos, cultura) y externo (mercado, regulaciones) de la organización.

- **Identificación de riesgos (identificar activos y amenazas)**: enumerar amenazas y vulnerabilidades que puedan afectar la confidencialidad, integridad y disponibilidad de los activos.

- **Análisis de riesgos (estimación de probabilidad e impacto)**: evaluar la probabilidad de ocurrencia de cada riesgo y su impacto potencial en los objetivos. El riesgo se concibe como la combinación de probabilidad e impacto de un evento adverso.

- **Evaluación de riesgos (priorización del riesgo):** comparar los niveles de riesgo obtenidos con criterios preestablecidos para priorizar las acciones; por ejemplo, mediante matrices de riesgo (bajo, medio, alto).

- **Tratamiento de riesgos (definir estrategias de tratamiento)**: decidir e implementar acciones correctivas, como mitigación (controles de seguridad), transferencia (seguros o contratos), aceptación (si el riesgo es bajo) o evitación (eliminar la actividad de alto riesgo).

- **Comunicación y monitoreo continuo**: informar y revisar periódicamente los riesgos y la eficacia de los controles. Este ciclo debe repetirse constantemente (gestión dinámica).

Por ejemplo, en la práctica, el riesgo puede estimarse con la fórmula **riesgo = probabilidad × impacto**, asignando valores cualitativos (alto/medio/bajo) o cuantitativos. Por ejemplo, si la probabilidad de un ataque es alta y su impacto financiero estimado es elevado, el riesgo será crítico y requerirá acciones inmediatas (como aplicar parches o capas de defensa adicionales).

Por ejemplo, en la etapa de la definición de estrategias de tratamiento del riesgo, entre las estrategias comunes en gestión de riesgos (según la definición estándar), se incluyen las siguientes:

- transferir el riesgo a terceros (por ejemplo, comprando seguros o contratos de garantía, u *outsourcing*).
- Evitar el riesgo eliminando la fuente o causa (por ejemplo, discontinuando una actividad riesgosa).
- Mitigar el riesgo reduciendo su probabilidad o impacto (implementando controles de seguridad, copias de seguridad, redundancia).

- Aceptar el riesgo (asumir el riesgo) conscientemente cuando su costo de mitigación excede el beneficio, manteniendo planes de contingencia.

La gestión del riesgo se basa en estándares internacionales, tales como ISO 27005 (ISO, 2022), ISO 22301 (ISO, 2019), ISO 27036 (ISO, 2021), ISO 31000 (ISO, 2018), NIST, etcétera, a partir de los cuales las organizaciones suelen elegir metodologías formales según su necesidad. Por ejemplo:

- la norma internacional ISO 31000 establece un marco de referencia para esta gestión sistemática. Según ISO 31000, la gestión de riesgos debe integrarse en toda la organización, apoyada en principios como la inclusión de las partes interesadas, el enfoque estructurado y la mejora continua.

- En seguridad de la información, la norma ISO 27005 ofrece una guía detallada para la evaluación de riesgos: identifica, analiza, evalúa y trata los riesgos de información.

- El **NIST RMF** propone un proceso de siete pasos para integrar seguridad y riesgo

(prepárate, categoriza la información, selecciona controles).

- NIST SP 800-53 implementa, evalúa, autoriza operaciones y monitorea continuamente.
- Igualmente, otras metodologías (como OCTAVE o NIST SP 800-30) ofrecen marcos para análisis basados en activos o amenazas.

En cualquier caso, la alta dirección debe definir el apetito de riesgo (nivel aceptable de riesgo) y criterios de clasificación, para equilibrar innovación con seguridad.

Análisis de impacto del negocio (BIA, *business impact analysis*)

El BIA es el proceso de análisis del impacto en el tiempo de una interrupción sobre la organización. Es un estudio que cuantifica los costos y las consecuencias de la interrupción de cada proceso crítico. Con el BIA, se identifican los componentes (sistemas, datos, personas) indispensables para la operación, se calculan pérdidas por tiempo de inactividad, y se establecen las prioridades de recuperación.

Consiste en identificar y clasificar los procesos de negocio según su criticidad: los procesos cuya interrupción causa un daño intolerable a corto plazo (por ejemplo, la plataforma de ventas online 24×7) tienen alta prioridad.

En resumen, el BIA establece qué servicios/productos son vitales y cuándo deben recuperarse. Es uno de los primeros pasos en el desarrollo de un sistema de gestión de continuidad del negocio (SGCN) basado en ISO 22301.

1. 2. BCP (business continuity plan o plan de continuidad del negocio). Estrategias de continuidad y pruebas

Continuidad del negocio y recuperación de desastres

La continuidad de negocio o *business continuity* se refiere a la capacidad de una organización para seguir operando ante incidentes críticos o desastres, lo que reduce el impacto en sus servicios y recupera rápidamente la operación normal.

El plan de continuidad del negocio (o BCP [*business continuity plan*]) es el conjunto de planes y procesos que aseguran que una organización pueda seguir operando durante y después de una interrupción grave.

La norma internacional ISO 22301 define los requisitos de un sistema de gestión de continuidad de negocio (SGCN). Según la norma ISO 22301:2019, un sistema de gestión de continuidad del negocio (SGCN) debe garantizar la operación de las funciones críticas ante crisis como desastres naturales, ciberataques, pandemias, etcétera.

Según ISO 22301:2019, este sistema ayuda a prevenir, prepararse, responder y recuperarse de eventos inesperados, lo que proporciona un marco práctico para mitigar daños y mantener un servicio continuo. En otras palabras, la continuidad de negocio busca la resiliencia operativa y la pronta recuperación ante cualquier interrupción (desde fallos tecnológicos hasta desastres naturales o ataques), lo cual garantiza que los procesos críticos sigan funcionando o que se reanuden en un tiempo aceptable.

En términos generales, la disciplina de continuidad (BCM) abarca tanto el plan de recuperación de desastres tecnológicos (DRP) como el plan de restablecimiento de

procesos críticos. La recuperación de desastres se define como la capacidad para responder a una interrupción de servicios tecnológicos y restaurar las funciones esenciales del negocio.

Un sistema de gestión de continuidad del negocio (SGCN), basado en ISO 22301, sigue pasos semejantes a otros sistemas de gestión.

Planificación: definir roles (comité de continuidad) y establecer la política de continuidad.

Análisis de impacto del negocio (BIA [*business impact analysis*]) y gestión de riesgos: hacer BIA y análisis de amenazas (naturales, humanas, técnicas). Determina los procesos críticos y el costo de sus interrupciones.

Estrategias de recuperación (o de continuidad): identificar soluciones para reducir tiempos de inactividad. Mediante la definición de recursos, por ejemplo, usar sitios y redes de respaldo alternativos, redundancias, replicación de datos en la nube o acuerdos con terceros, sitios alternos, etcétera. Se establecen los tiempos objetivo (RTO/RPO). Los objetivos de recuperación (RTO, RPO), para cada proceso crítico, se definen como métricas:

- **RTO** (*recovery time objective*). Tiempo máximo tolerable de interrupción para el proceso.

- **RPO** (*recovery point objective*). Máxima pérdida de datos tolerable (por ejemplo, último *backup*) antes de que se considere inaceptable.

Desarrollo del plan de continuidad y documentarlo (BCP/DRP)

Una vez definidos los objetivos y las estrategias, se documentan planes formales (BCP/DRP) que detallan acciones concretas: notificación de incidentes, roles y responsabilidades, procedimientos de conmutación por error, etcétera. Son procedimientos detallados (planes de contingencia) para restablecer operaciones, servicios y funciones críticas. Por ejemplo: listas de verificación, comunicaciones de emergencia, copias de seguridad, etcétera.

Pruebas y mantenimiento: estos planes deben probarse y revisarse periódicamente mediante simulacros y auditorías para asegurar su eficacia. Se formalizan simulaciones

regulares del plan, revisión de vulnerabilidades y ajuste de procesos según resultados. Por ejemplo:

- simular escenarios (pruebas de desastre) para verificar el plan;
- capacitar al personal:
- actualizar el plan según cambios en la organización o los riesgos.

Mejora continua: adicionalmente, la mejora continua (lecciones aprendidas y ajustes tras cada prueba o incidente) es un requisito del estándar ISO 22301.

En resumen, un programa de continuidad bien implementado permite reducir el tiempo de inactividad y asegurar la resiliencia operativa ante eventos inesperados. En el SGCN se coordinan acciones preventivas y reactivas, lo que garantiza tanto **prevención** (reducción de probabilidad) como **recuperación rápida** (reducir impacto).

Las organizaciones públicas (transporte, salud, servicios básicos) suelen necesitar un SGCN certificado.

1. 3. DRP (disaster recovery plan o plan de recuperación desde el desastre): cómo restaurar la infraestructura de TI y los datos después de un incidente

La recuperación de desastres se define como la capacidad para responder a una interrupción de servicios tecnológicos y restaurar las funciones esenciales del negocio.

Un plan de recuperación ante desastres (DRP) es un enfoque estructurado que describe procedimientos y herramientas para restaurar sistemas de TI, datos y operaciones críticos después de un ciberataque, un desastre natural u otra interrupción. Ayuda a garantizar la continuidad del negocio definiendo medidas para reducir el tiempo de inactividad y salvaguardar los activos sensibles.

Un plan de recuperación ante desastres (DRP) es un conjunto de procedimientos y estrategias documentadas que permiten a una organización restaurar su infraestructura de TI y datos críticos después de una interrupción o evento catastrófico. Su objetivo principal es reducir el tiempo de inactividad y las pérdidas de datos para garantizar la continuidad del negocio.

A continuación, se describen los pasos claves para restaurar la infraestructura de TI y los datos, que deben estar incluidos en un DRP bien diseñado.

1 Fase de preparación (antes del incidente)

La restauración exitosa depende de la preparación previa.

- **Análisis de riesgos y del impacto en el negocio (BIA)**: identificar las amenazas potenciales (ciberataques, desastres naturales, fallos de *hardware*) y los sistemas, datos y aplicaciones más críticos para el negocio. El BIA determina el impacto de una interrupción en cada uno de ellos.
- **Establecimiento de objetivos de recuperación**: definir dos parámetros claves**,** es decir, el RTO (objetivo de tiempo de recuperación), el tiempo máximo aceptable para que una aplicación o servicio se restablezca y vuelva a funcionar después de un desastre. Y, por otra parte, definir el RPO (objetivo de punto de recuperación), es decir, la cantidad máxima de datos que se puede permitir perder, lo que determina la frecuencia con la que se deben hacer las copias de seguridad.

- **Estrategia de copias de seguridad**: aplicar una política de respaldo sólida. Esto incluye la selección de tecnologías (cinta, disco, nube), la frecuencia de los respaldos y la ubicación de las copias (preferiblemente fuera de las instalaciones).
- **Replicación de datos y sistemas**: para los datos y las aplicaciones más críticos, usar la replicación a un sitio secundario. Las soluciones en la nube, como la recuperación como servicio (DRaaS), ofrecen opciones flexibles y escalables para este fin.
- **Documentación del DRP**: crear un documento detallado que incluya procedimientos paso a paso, roles y responsabilidades, y la información de contacto de las personas claves (equipo de respuesta, proveedores, etcétera).
- **Pruebas del DRP**: hacer simulacros y pruebas periódicas para validar que el plan funciona según lo esperado y que el personal sabe cómo actuar en caso de emergencia.

2 Fase de respuesta (durante el incidente)

El DRP se activa en el momento de la interrupción para mitigar los daños.

- **Activación del plan**: declarar el desastre y activar formalmente el DRP.
- **Notificación y comunicación**: informar a los equipos de respuesta y a las partes interesadas, siguiendo los protocolos de comunicación establecidos.
- **Evaluación inicial**: determinar el alcance y la naturaleza del incidente para priorizar los esfuerzos de recuperación.
- **Evaluación de daños**: valorar la infraestructura afectada y el grado de pérdida de datos.

3 Fase de restauración (después del incidente)

Este es el proceso de volver a la normalidad, siguiendo los procedimientos documentados.

Recuperación de la infraestructura

- **Restaurar en un sitio alterno**: si se usa un sitio de recuperación (propio o en la nube), se activa la infraestructura de respaldo para restablecer los servicios más críticos.

- **Reconstruir sistemas**: si la infraestructura principal es recuperable, se comienza con la restauración de los servidores, la red y las aplicaciones en un orden de prioridad predeterminado.

Restauración de los datos

- **Recuperar desde las copias de seguridad**: restaurar los datos desde las copias de seguridad a un estado anterior al incidente, según el RPO establecido.
- **Sincronizar datos**: si se utilizaba replicación, se sincronizan los datos del sitio secundario al primario una vez que la infraestructura se haya restaurado.
- **Verificación y validación**: confirmar que todos los sistemas y datos han sido restaurados correctamente y que las aplicaciones funcionan como se espera.
- **Cambio a operaciones normales**: una vez que se verifique la integridad de todos los sistemas, se procede a cambiar nuevamente a la infraestructura principal, si corresponde, y a las operaciones regulares.

4 **Fase de postrecuperación**

Después de que los sistemas están en funcionamiento, el trabajo continúa.

- **Análisis *post mortem***: hacer una revisión completa del incidente y del proceso de recuperación.
- **Actualización del DRP**: con base en los aprendizajes del incidente, actualizar el DRP y mejorar los procedimientos de recuperación.
- **Mitigación de riesgos futuros**: aplicar medidas correctivas y preventivas para evitar que un incidente similar vuelva a ocurrir.

1. 4. KRI (indicadores claves de riesgo)/KPI (indicadores claves de rendimiento) en el análisis de riesgo y continuidad

En el análisis de riesgos y la gestión de la continuidad del negocio, los indicadores clave de riesgo (KRI) y los indicadores clave de rendimiento (KPI) son herramientas complementarias, pero con propósitos distintos. Los KRI alertan sobre la posible materialización de un riesgo,

mientras que los KPI miden el desempeño de las operaciones o la eficacia de los controles.

KRI (indicador clave de riesgo)

Un KRI es una métrica predictiva que indica la probabilidad de que un riesgo supere los límites aceptables de la organización. Su objetivo es servir como una señal de alerta temprana para tomar medidas preventivas antes de que un problema ocurra.

Características

- **Preventivo y proactivo**: se centra en la probabilidad de un evento futuro y sus posibles consecuencias negativas.
- **Cuantifica el riesgo**: permite medir la exposición o vulnerabilidad de la organización ante amenazas potenciales.
- **Define umbrales**: se establecen límites que, al ser superados, requieren una respuesta o corrección.

Ejemplos en riesgo y continuidad

- **Ciberseguridad**: número de intentos de acceso no autorizados o de ataques de phishing.
- **Operacional**: rotación de personal o frecuencia de fallos en un sistema.
- **Financiero**: cobertura diaria del flujo de caja o dependencia de financiación externa.
- **Continuidad del negocio**: número de horas fuera de servicio de un sistema clave para la operación.

KPI (indicador clave de rendimiento)

Un KPI es una métrica que mide la eficacia con la que una organización, un equipo o un proceso está logrando un objetivo de negocio. Su función es evaluar el desempeño, el progreso hacia los objetivos y las tendencias a lo largo del tiempo.

Características

- **Reactivo y retrospectivo**: mide el rendimiento pasado o presente para evaluar la consecución de metas.

- **Mide el éxito**: se centra en el logro de objetivos, como ventas, productividad o satisfacción del cliente.

- **Establece métricas**: usa medidas específicas y cuantificables para evaluar el desempeño con precisión.

Ejemplos en riesgo y continuidad

Continuidad del negocio

- **Objetivo de tiempo de recuperación (RTO)**: el tiempo máximo aceptable para recuperar una función crítica después de una interrupción.
- **Objetivo de punto de recuperación (RPO)**: la cantidad máxima de datos que se pueden perder, medida en tiempo, durante una interrupción.
- **Costo del tiempo de inactividad**: el impacto financiero de la interrupción del servicio.
- **Gestión de riesgos**: número de riesgos identificados y mitigados, y el tiempo de mitigación.

Uso conjunto de KRI y KPI

En la gestión de la continuidad del negocio, la combinación de KRI y KPI ofrece una supervisión integral y estratégica.

- **Complementariedad**: los KRI advierten sobre un posible aumento de un riesgo (por ejemplo, alta rotación de personal), mientras que los KPI miden el impacto del control (por ejemplo, tiempo de recuperación después de una interrupción).

- **Alerta y evaluación**: un KRI puede dar la señal de alerta sobre un evento adverso inminente (por ejemplo, aumento de ciberataques). Posteriormente, un KPI evalúa la eficacia de la respuesta de continuidad al medir el RTO real, el RPO real y el costo total del incidente.

- **Mejora continua**: los KRI pueden informar sobre áreas de riesgo que necesitan más atención, mientras que los KPI permiten medir las mejoras implementadas. Por ejemplo, si un KRI muestra un riesgo creciente de falla tecnológica, un KPI puede evaluar el rendimiento del plan de mitigación tras su implementación.

CONTINUAR

Unidad 2: Terceros y aspectos legales (AR)

Unidad 2: Terceros y aspectos legales (AR)

La gestión de riesgos de terceros es un proceso para identificar, evaluar y mitigar los riesgos de ciberseguridad que presentan los proveedores, contratistas, socios y otros terceros que tienen acceso a los datos o sistemas de una empresa.

- **Aumento del riesgo**: el uso de terceros amplía la superficie de ataque de una organización, lo que aumenta el riesgo de filtraciones de datos, vulnerabilidades y daños a la reputación.

- **Necesidad de un control estricto**: es vital que las empresas establezcan requisitos de seguridad para los proveedores, evalúen sus prácticas y los monitoreen continuamente para garantizar el cumplimiento de las normas de seguridad.

Aspectos legales en Argentina (AR)

La gestión de la seguridad de la información y de los terceros en Argentina debe cumplir con un marco legal específico, que incluye la ley de Protección de Datos Personales.

- **Ley 25326 de protección de datos personales**: esta ley garantiza el derecho a la protección de los datos personales. Establece que toda persona tiene derecho a que sus datos personales sean rectificados, actualizados, suprimidos o confidencializados.

- **Rol de la AAIP**: la Agencia de Acceso a la Información Pública (AAIP) es la autoridad de control que aplica la Ley de Protección de Datos Personales y garantiza los derechos de los titulares de los datos.

- **Obligación de seguridad**: la ley impone a los responsables y usuarios de bases de datos la obligación de implementar medidas de seguridad técnicas, administrativas y físicas para proteger los datos personales contra accesos, pérdidas, alteraciones o destrucciones no autorizadas.

- **Responsabilidad en el tratamiento de datos por terceros**: si se utilizan terceros para el tratamiento de datos personales, la empresa contratante debe asegurarse de que el tercero cumple con las normativas de seguridad.

- **Consecuencias del incumplimiento**: la falta de cumplimiento de las normativas puede acarrear sanciones, multas, procesos legales y daños a la reputación, incluso si la infracción se origina en un tercero.

- **Regulaciones sectoriales**: adicionalmente, sectores como el bancario, regulado por el Banco Central (BCRA), tienen normativas de

seguridad de la información específicas que complementan la legislación nacional.

2. 1. Riesgo de proveedores y acuerdos de seguridad

Gestión de riesgos de proveedores y terceros

La **gestión de riesgos de terceros** (*third party risk management* [TPRM]), o gestión de proveedores, se centra en identificar y reducir los riesgos asociados al uso de servicios y bienes externos. Aborda las amenazas derivadas de la dependencia de proveedores, socios, contratistas y cualquier entidad externa. Abarca desde proveedores de materias primas o consultores hasta servicios tecnológicos subcontratados.

Cada relación con un tercero puede introducir vulnerabilidades; por ejemplo, un proveedor de servicios en la nube con mala seguridad podría filtrar datos sensibles. La importancia de esta gestión radica en evitar daños severos: muchas empresas han sufrido pérdidas económicas y reputacionales por incidentes originados en proveedores externos.

En el entorno actual, las organizaciones dependen de múltiples proveedores (*cloud*, TI, logística, servicios profesionales, etcétera), por lo que un fallo externo puede causar interrupciones devastadoras. Por ejemplo, una caída de un proveedor de nube afectaría los sistemas internos, o un ataque al *software* de un tercero podría comprometer datos sensibles.

Normas como **ISO/IEC 27036** ofrecen directrices específicas para las relaciones con proveedores, orientando sobre la evaluación y tratamiento de los riesgos de información al adquirir bienes y servicios.

En esencia, la gestión de terceros busca garantizar que acuerdos con proveedores incluyan criterios de seguridad y continuidad (SLA, evaluaciones de cumplimiento, planes de contingencia).

Sin un programa formal de riesgos de terceros, la dependencia externa genera **vulnerabilidades** operativas y de seguridad. La TPRM utiliza herramientas y marcos de evaluación para garantizar la **resiliencia** operativa y

financiera ante adversidades vinculadas a terceros. En la práctica, un programa para gestionar riesgos de terceros implementa controles a lo largo de todo el ciclo de vida del proveedor en la empresa. A continuación, se presentan algunos ejemplos.

- **Debida diligencia previa**: evaluar la solvencia financiera y las prácticas de seguridad del proveedor antes de contratar.
- **Inventario y clasificación**: listar todos los proveedores y clasificarlos por nivel de criticidad.
- **Evaluación inicial**: revisar controles de seguridad del proveedor, cumplimiento normativo y continuidad operativa. Evaluar la criticidad de sus servicios y sus controles de seguridad, evaluar el riesgo.
- **Tratamiento del riesgo. Planes de contingencia**: tener proveedores alternativos o planes de respaldo si el tercero falla.
- **Monitoreo continuo**: hacer auditorías regulares, reevaluaciones y seguimientos periódicos o tras cambios o incidentes.

- **Acuerdos contractuales**: incluir cláusulas que exijan requisitos y niveles mínimos de seguridad, notificación de brechas, confidencialidad, cumplimiento normativo y planes de recuperación.

Por ejemplo, se segmentan los proveedores según su nivel de riesgo/criticidad (alto, medio, bajo) para priorizar recursos. Aquellos de **alto riesgo** (nivel 1) —que manejan datos sensibles o procesos críticos— requieren diligencia debida exhaustiva (revisiones frecuentes, auditorías *in situ*, cláusulas contractuales estrictas).

Entre los **tipos de riesgos de terceros**, destacan los que se describen a continuación.

- **Financieros**: si un proveedor afronta problemas económicos, podría interrumpir la cadena de suministro.
- **Reputacionales**: un escándalo o brecha de seguridad en el tercero afecta la imagen de la empresa.
- **Regulatorios/cumplimiento**: si el tercero incumple leyes (por ejemplo, protección de

datos), la empresa puede enfrentarse a sanciones legales.

- **Operativos**: interrupciones en proveedores clave (desastre natural, fallos de producción) pueden paralizar las operaciones.

- **Estratégicos**: falta de alineamiento entre objetivos de la empresa y el proveedor puede generar incompatibilidades o ineficiencias.

Con un buen programa de gestión de terceros, se mitigan riesgos de *supply chain*, se mejora la visibilidad de vulnerabilidades externas y se protege la cadena de valor de la organización.

2. 2. Ley 25326 y principios de protección de datos

La Ley 25326 de la República Argentina, conocida como la Ley de Protección de Datos Personales, busca garantizar el derecho al honor, la intimidad y el acceso a la información de las personas. Establece un marco legal para el tratamiento de datos personales en archivos, registros y bases de datos, ya sean públicos o privados.

Esta normativa se fundamenta en principios básicos que deben ser respetados por quienes manejan datos personales.

Principios de la Ley 25326

La ley establece una serie de principios esenciales para el manejo adecuado de los datos personales.

- **Principio de legalidad y lealtad**: los datos deben ser obtenidos y tratados de manera lícita, justa y sin engaños. Es decir, se debe informar al titular del dato sobre la finalidad y las condiciones del tratamiento de su información personal.

- **Principio de finalidad**: los datos deben ser recolectados con fines específicos, legítimos y explícitos. No pueden ser usados para propósitos distintos a los que motivaron su obtención.

- **Principio de calidad**: los datos deben ser veraces, adecuados, pertinentes y no excesivos en relación con el fin para el que se recopilaron. También deben ser actualizados y, de ser necesario, eliminados o corregidos.

- **Principio de consentimiento**: por regla general, el tratamiento de los datos personales requiere el consentimiento libre, expreso e informado del titular. Existen excepciones, como cuando los datos provienen de fuentes de acceso público o cuando una ley así lo dispone.

- **Principio de seguridad**: quienes manejan datos personales deben adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de la información. Esto evita su alteración, pérdida, consulta o tratamiento no autorizado.

- **Principio de confidencialidad**: el responsable de la base de datos y cualquier persona que intervenga en el tratamiento de los datos personales tiene la obligación de guardar secreto o confidencialidad.

- **Principio de acceso**: el titular de los datos tiene derecho a solicitar y obtener información sobre sus datos personales, lo que incluye la finalidad de la base de datos, quién es el responsable y cuál es su domicilio.

Derechos del titular de los datos

La Ley 25326 garantiza el ejercicio de derechos específicos a los titulares de los datos:

- **derecho de acceso**. Permite a la persona conocer los datos que figuran sobre ella en una base de datos. Este derecho puede ejercerse de forma gratuita a intervalos de seis meses, salvo interés legítimo.
- **Derecho de rectificación**: el titular puede solicitar la corrección de su información si esta fuera inexacta, incompleta o estuviera desactualizada.
- **Derecho de supresión o eliminación**: permite solicitar la eliminación total o parcial de los datos personales que no sean necesarios para el fin para el que fueron recabados.

Marco regulatorio y autoridad de aplicación

La ley se complementa con el Decreto reglamentario 1558/2001. La autoridad de aplicación en Argentina es la Agencia de Acceso a la Información Pública (AAIP),

encargada de fiscalizar el cumplimiento de la ley y mantener el Registro Nacional de Bases de Datos Personales.

Contexto y actualización

La Ley 25326 fue sancionada en el año 2000, influenciada por la normativa europea de la época. Desde 2022, se ha abierto un debate para la posible actualización de la ley, buscando adaptarla a los estándares internacionales más modernos, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.[1]

[1] Reglamento de la Unión Europea 679 de 2016 [Parlamento Europeo]. Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). 27 de abril de 2016.

2. 3. Transferencias, registros, privacidad por diseño

En el contexto de la seguridad de la información y la gestión de riesgos en Argentina, los conceptos de **transferencias de datos, registros de datos y privacidad por diseño** son pilares fundamentales para garantizar el cumplimiento de la Ley de Protección de Datos Personales (Ley 25326) y asegurar la protección de la privacidad.

Transferencias de datos personales

Las transferencias de datos personales se refieren a la comunicación de datos entre el responsable del tratamiento y un tercero, que puede estar dentro o fuera del país.

Transferencias nacionales

- **Finalidad**: solo están permitidas para el cumplimiento de fines legítimos tanto para quien cede los datos como para quien los recibe.
- **Consentimiento**: generalmente, se requiere el consentimiento previo del titular de los datos. La transferencia debe ser transparente para el individuo.

Transferencias internacionales

- **Países con «adecuado nivel de protección»**: la ley argentina establece que las transferencias internacionales solo están

permitidas a países que ofrecen un nivel de protección comparable al de Argentina.

- **Excepciones**: existen excepciones para transferir datos a países sin el nivel de protección adecuado, aunque bajo circunstancias muy específicas.

- **Responsabilidad**: el responsable del tratamiento debe asegurarse de que el tercero receptor en el extranjero cumpla con la normativa argentina.

Registros de datos

El registro de datos es una obligación clave para los responsables de bases de datos, ya sean públicas o privadas.

Registro Nacional de Bases de Datos

En Argentina, la Agencia de Acceso a la Información Pública (AAIP) administra el Registro Nacional de Bases de Datos, donde deben inscribirse los responsables y sus bases de datos personales.

Obligatoriedad: esta inscripción es un deber legal y su principal objetivo es garantizar el derecho de habeas data de los ciudadanos, ofreciendo transparencia sobre quién maneja sus datos y con qué propósito.

Información del registro: las inscripciones deben detallar la finalidad de la base de datos y los datos de contacto del responsable.

Inspecciones: el registro permite a la AAIP supervisar el cumplimiento de la normativa y asegura que se cumplan los estándares de seguridad necesarios.

Privacidad por diseño (*privacy by design*)

La privacidad por diseño es una metodología de desarrollo que integra la protección de datos en la arquitectura de los sistemas y procesos desde la etapa inicial de diseño.

Enfoque proactivo

A diferencia de un enfoque reactivo, que trata los problemas de privacidad después de que surgen, la privacidad por diseño es preventiva.

Integración en el ciclo de vida

La protección de datos debe considerarse a lo largo de todo el ciclo de vida de un producto, servicio o sistema.

Principios claves (según la doctora Ann Cavoukian, creadora del concepto)

- **Proactivo, no reactivo**: anticipa y previene eventos de privacidad antes de que sucedan.
- **Privacidad por defecto**: la configuración predeterminada de un sistema debe ser la más protectora de la privacidad.
- **Integración en el diseño**: la privacidad debe estar integrada en el diseño, no ser un complemento.
- **Funcionalidad completa**: el enfoque no debe sacrificar la funcionalidad en aras de la privacidad.
- **Seguridad de extremo a extremo**: la protección de los datos debe ser continua.
- **Visibilidad y transparencia**: la política de privacidad debe ser clara para los usuarios.

- **Respeto por la privacidad del usuario**: poner los intereses del individuo en primer lugar.

Relevancia en Argentina

Adoptar la privacidad por diseño permite a las organizaciones argentinas cumplir de manera más robusta con las obligaciones de seguridad y transparencia establecidas en la Ley 25326.

Implicaciones prácticas

Para una organización que maneja datos personales en Argentina, esto significa lo siguiente:

- **evaluar riesgos**. Analizar los riesgos de privacidad y seguridad antes de cualquier transferencia de datos, tanto a nivel nacional como internacional.

- **Garantizar la protección en las transferencias**: asegurarse de que los terceros a los que se transfieren los datos cumplan con los mismos estándares de seguridad requeridos por la ley argentina.

- **Cumplir con los registros**: inscribir obligatoriamente las bases de datos en el registro de la AAIP para operar de forma transparente y legal.

- **Adoptar la privacidad por diseño**: diseñar sistemas y procesos pensando en la privacidad desde el inicio, lo que reduce la recolección de datos y asegura controles de seguridad robustos.

2. 4. Auditorías y cláusulas contractuales

Sumando a lo mencionado en las secciones anteriores, se pueden agregar normas Internacionales.

GDPR (Reglamento General de Protección de Datos)

El Reglamento general de protección de datos (RGPD) es una ley integral de protección de datos aprobada por la Unión Europea (UE). Establece requisitos estrictos para la protección de datos en la UE.

El Reglamento general de protección de datos (RGPD), que entró en vigor el 25 de mayo de 2018, es una ley integral de privacidad de datos, que establece un marco para la recopilación, el tratamiento, el almacenamiento y la transferencia de datos personales. Exige que todos los datos personales se procesen de forma segura, e incluye multas y sanciones para las empresas que no cumplan con estos requisitos. También proporciona a los individuos una serie de derechos en relación con sus datos personales.

A medida que la tecnología avanza y la recopilación de datos se hace más frecuente, la privacidad de datos se ha puesto en el punto de mira. En el momento de su aprobación, el RGPD era la normativa de privacidad de datos más completa. Armonizaba las distintas normativas de protección de datos de toda la Unión Europea (UE). También amplió el alcance de esas normas para aplicarlas a las organizaciones no pertenecientes a la UE en caso de que trataran con datos personales recopilados en la UE.

El RGPD se aplica a cualquier empresa u organización, independientemente de su ubicación geográfica, si la empresa u organización ofrece bienes y servicios a personas en la UE o supervisa su comportamiento dentro de la UE.

Ejemplo: dice que las brechas de seguridad, incluidas las provocadas por SQLi, XSS y CSRF, deben ser notificadas a las autoridades.

«Datos personales» según la RGPD

El RGPD amplió el alcance de lo que se consideraba datos personales para incluir cualquier información relacionada con una persona física identificable. Esto incluye detalles que son obviamente personales, como el nombre y la dirección de alguien, pero también cualquier otra información que pueda utilizarse para identificarlo, incluida su dirección IP y ciertos identificadores de *cookies* asociados a una sesión de navegación web.

Requisitos del RGPD para los controladores de datos y los procesadores de datos

El RGPD define a los controladores de datos como las entidades que toman decisiones sobre los medios y fines para los que se recopilan y procesan los datos personales, y define a los procesadores de datos como las entidades que procesan datos personales, normalmente en nombre de un controlador de datos.

El RGPD también establece siete principios clave sobre cómo deben tratar los datos personales los controladores y procesadores de datos:

- Legalidad, equidad y transparencia.
- Limitación de la finalidad.
- Minimización de datos.
- Precisión.
- Limitación de almacenamiento.
- Integridad y confidencialidad (seguridad).
- Responsabilidad.

Además de describir estos principios en detalle, el RGPD requiere que los controladores y procesadores de datos tomen varias acciones específicas. Entre algunas de ellas, se incluyen:

- Mantenimiento de registros. Los procesadores de datos deben mantener registros de sus actividades de procesamiento.
- Medidas de seguridad: los procesadores y controladores deben utilizar y probar

periódicamente las medidas de seguridad adecuadas para proteger los datos que recopilan y procesan.

- Notificación de fugas de datos: los controladores de datos que sufran una fuga de datos personales tienen que notificarlo a las autoridades competentes en un plazo de setenta y dos horas, con algunas excepciones. Por lo general, también tienen que notificar a las personas cuyos datos personales se hayan visto afectados por la fuga.

- Delegado de protección de datos (DPO): es posible que las empresas que procesan datos tengan que contratar a un delegado de protección de datos (DPO). El DPO dirige y supervisa todos los esfuerzos de cumplimiento del RGPD.

Todos los requisitos para los controladores y procesadores de datos se describen en el RGPD.

Derechos tienen los sujetos de datos en virtud del RGPD

El RGPD define al sujeto de datos como una persona física identificada o identificable. Los sujetos de datos tienen los

siguientes derechos:

- **Derecho a ser informado**. Los sujetos de datos deben recibir información fácil de entender sobre cómo se recopilan y tratan sus datos personales.

- **Derecho a la portabilidad de los datos**: los sujetos de datos pueden transferir sus datos de un controlador de datos a otro.

- **Derecho de acceso**: los sujetos de datos tienen derecho a obtener una copia de los datos personales recopilados.

- **Derecho de rectificación**: los sujetos de datos pueden corregir los datos inexactos que haya sobre ellos.

- **Derecho de supresión**: los sujetos de datos pueden solicitar la supresión de sus datos (también llamado derecho al olvido).

- **Derecho a limitar el procesamiento**: en determinadas circunstancias, los sujetos de datos pueden limitar la forma en la que se procesan sus datos personales.

- **Derecho a oponerse**: los sujetos de datos tienen derecho a oponerse al procesamiento de sus datos personales y, en determinadas circunstancias, el controlador de datos o el procesador de datos estarán obligados a cumplir con la oposición del sujeto de datos.

- **Derecho a oponerse al procesamiento automatizado**: los sujetos de datos pueden oponerse a una decisión que les afecte jurídicamente y que esté basada únicamente en un procesamiento de datos automatizado.

Sanciones por infringir el RGPD

El RGPD describe las multas que se impondrán a las empresas que infrinjan sus políticas. El RGPD establece dos niveles de multas, cada uno de los cuales corresponde a una categoría de infracción diferente.

- **Primer nivel**: una infracción tiene como consecuencia una multa máxima de 10 millones de euros o del 2 % de los ingresos anuales de la empresa en todo el mundo, el importe que sea superior.

- **Segundo nivel**: una infracción tiene como consecuencia una multa máxima de 20 millones de euros o del 4 % de los ingresos anuales de la empresa en todo el mundo, el importe que sea superior.

Además de estas multas, los sujetos de datos pueden solicitar una indemnización por daños y perjuicios cuando una empresa infrinja el RGPD.

HIPAA (Health Insurance Portability and Accountability Act)

La HIPAA es una ley federal que regula la manera en que determinadas organizaciones implicadas en la prestación de atención médica manejan y protegen la información de salud. La **ley de Transferencia y Responsabilidad de Seguros Médicos (HIPAA)** es una ley federal que regula el tratamiento y la seguridad de la información de salud. La HIPAA ayuda a garantizar la protección de la información de salud, al requerir controles de seguridad para la información de salud electrónica y al ordenar prácticas de privacidad. Obliga a proteger la información médica en EE. UU. Por ejemplo, Inyecciones SQL en bases de datos médicas pueden violar esta regulación.

La HIPAA tiene un impacto en dos tipos principales de organizaciones: las entidades cubiertas, como los proveedores de atención médica, los planes de salud y los centros de información de salud, y los socios empresariales de las entidades cubiertas, como las empresas de facturación, los proveedores de registros médicos electrónicos (HCE), los consultores o los proveedores de TI.

Información de salud protegida (PHI)

La **información de salud protegida (PHI)** es cualquier información de salud identificable individualmente relacionada con la prestación de atención médica que las entidades cubiertas y los socios empresariales crean, reciben, almacenan o transmiten. La PHI es un tipo de **información de identificación personal (PII)**, que consiste en datos que pueden utilizarse para identificar a una persona.

A continuación, se indican los campos de datos que pueden ser PHI si los procesa una entidad cubierta o un socio

empresarial y en la medida en que los datos estén asociados a la prestación de atención médica:

- nombre.
- Dirección.
- Huellas digitales.
- Reconocimiento facial.
- Número de seguridad social.
- Fecha de nacimiento.
- Información sobre seguro médico.
- Números de registro médico.
- Números de cuenta.
- Direcciones IP.
- Registros de facturación.

Es importante destacar que la PHI puede presentarse en varias formas, desde datos escritos a orales o electrónicos.

Ejemplo: supongamos que Michael visita a un médico general por primera vez y que el consultorio del médico registra el nombre y la dirección de Michael, toma los datos de su seguro médico y solicita verbalmente sus registros

médicos a su proveedor anterior. Todos estos datos escritos y orales se consideran PHI y se deben proteger.

Ahora, supongamos que Michael tiene una cita de telemedicina con este mismo médico la siguiente semana. La información sobre las actividades en línea de Michael que revelan los detalles sobre su cita de telemedicina también puede considerarse PHI, aunque sea información electrónica y no escrita u oral.

Norma de privacidad y la norma de seguridad de la HIPAA

La **norma de privacidad de la HIPAA** requiere que las entidades cubiertas y los socios empresariales incorporen salvaguardias y políticas de privacidad adecuadas para proteger la PHI. Existen normas estrictas sobre lo que una organización puede hacer con la PHI sin el consentimiento de la persona y la norma de privacidad otorga a las personas el derecho a saber cómo se usan sus datos o a solicitar correcciones.

La **norma de seguridad de la HIPAA** exige salvaguardias administrativas, físicas y técnicas para manejar adecuadamente la PHI de manera electrónica, desde garantizar el acceso seguro a las instalaciones y el control de los dispositivos, designar personal de seguridad y aplicar la

formación de la fuerza de trabajo, hasta hacer análisis de riesgos.

¿Por qué es importante la HIPAA?

Las normas de seguridad y privacidad de la HIPAA son importantes para garantizar que la información de salud de las personas esté debidamente protegida, al mismo tiempo que permite el flujo de información de salud necesario para prestar y promover una atención médica de alta calidad, y para proteger la salud y el bienestar públicos. Estas normas son especialmente importantes dada la diversidad del mercado de la atención médica, la variedad de usos y divulgaciones que deben abordarse, así como la afluencia de nuevas tecnologías innovadoras en el campo de la atención médica, tales como la telemedicina, la terapia remota, los registros de salud electrónicos, la supervisión de la salud mediante dispositivos y la atención asistida por IA. En concreto, cada una de estas nuevas tecnologías innovadoras conlleva sus propios retos en cuanto a seguridad y privacidad, que las organizaciones deben abordar conforme a las normas de seguridad y privacidad de la HIPAA.

Incumplimientos habituales de la HIPAA

Las infracciones de la HIPAA pueden resultar en fuertes sanciones y acciones legales. Algunas de las infracciones más comunes incluyen:

- fuga de datos por no proteger adecuadamente la PHI, que incluye el robo de PHI con fines lucrativos o personales.
- Acceso no autorizado, divulgación o uso inapropiado de los datos de PHI.
- Formación inadecuada y deficiente de los empleados que manejan la PHI.
- No notificar adecuadamente a las autoridades y a las personas pertinentes tras una fuga de datos.
- No se tienen las salvaguardias físicas, técnicas y administrativas necesarias.

Imagina que el médico de Michael dejara el formulario del paciente con el nombre, la fecha de nacimiento, el número de seguridad social y las preocupaciones médicas de Michael en la sala de espera durante veinticuatro horas, donde cualquier paciente o miembro del personal tuviera acceso a este. Luego, imagina que el médico carga la información de salud de Michael a un portal en línea, que no estaba

protegido con una contraseña. Ambas situaciones son ejemplos de incumplimiento de la HIPAA.

Penalizaciones por infringir la HIPAA

Las penalizaciones por incumplimiento de la HIPAA son importantes y pueden oscilar entre 100 USD por infracción y 1 500 000 USD por disposición anualmente. La Oficina de Derechos Civiles (OCR) clasifica las infracciones de la HIPAA con base en la gravedad y la negligencia intencionada.

- **Nivel I**: **desconocimiento de la infracción**. La entidad no es consciente que ha incumplido con la normativa HIPAA y las sanciones oscilan entre 100 USD y 50 000 USD por infracción, con una sanción máxima de 25 000 USD al año.

- **Nivel II**: **causa razonable**. La entidad no actuó con negligencia deliberada. Las sanciones por infracciones del nivel II oscilan entre los 1000 USD y los 50 000 USD por caso, con una sanción máxima de 100 000 USD al año.

- **Nivel III: negligencia deliberada que se corrige en un plazo de treinta días de haberse descubierto**. Las sanciones pueden

oscilar entre los 10 000 USD y los 50 000 USD por infracción, y pueden alcanzar un máximo de 250 000 USD al año.

- **Nivel IV**: **negligencia deliberada que no se corrige en treinta días**. Al ser el nivel más grave, las sanciones por infracciones del nivel IV pueden alcanzar hasta 1 500 000 USD por disposición cada año.

¿Cómo los proveedores de la nube aseguran el cumplimiento de la HIPAA?

Los proveedores de servicios en la nube deben firmar con sus clientes un acuerdo de asociación empresarial (BAA, por sus siglas en inglés) conforme a la HIPAA para poder crear, recibir, mantener o transmitir la PHI. Un BAA requiere que el proveedor de servicios en la nube proporcione protecciones adecuadas para la PHI, y que realice análisis de riesgos para identificar posibles vulnerabilidades. También puede incluir instrucciones específicas sobre la disponibilidad de los datos, copias de seguridad, recuperación ante desastres y retención de datos.

Los proveedores de servicios en la nube también son responsables de cualquier divulgación no autorizada de la

PHI, o de no proteger la PHI o de informar a las autoridades pertinentes sobre una fuga de datos.

Buenas prácticas para cumplir con la HIPAA

Estas son seis recomendaciones para garantizar el cumplimiento de la HIPAA:

- identificar los riesgos únicos y crear políticas para gestionarlos, incluidos los programas de formación y políticas establecidas de notificación de infracciones.
- Supervisar el uso de la PHI y reducir el acceso a los datos protegidos siempre que sea posible.
- Hacer análisis de riesgos periódicos y exhaustivos, incluidas auditorías de seguridad y cumplimiento.
- Incorporar salvaguardias físicas y digitales, como protección por contraseña, restricciones de uso de dispositivos y medios, y controles de acceso.

- Incorporar salvaguardias técnicas, como controles de auditoría, encriptación y políticas de autenticación.

- Implementar procesos e infraestructuras de seguridad para ayudar a los proveedores de confianza a manejar adecuadamente la PHI.

PCI DSS (Payment Card Industry Data Security Standard)

- Exige medidas para prevenir vulnerabilidades en sistemas que procesan datos de tarjetas de crédito.

Ley nacional de protección de datos personales: en muchos países (como Argentina), la ley protege la información personal de los ciudadanos.

Responsabilidades de las empresas

- Implementar medidas de seguridad preventivas.
- Documentar y reportar incidentes.
- Cumplir con auditorías de seguridad periódicas.

CONTINUAR

Referencias

Ley 25326 de 2000. Ley de Protección de los Datos Personales (hábeas data). 30 de octubre de 2000. D.O. No. 29517 (B.O. 2/11/2000).

Organización Internacional de Normalización. (2018). *Gestión del riesgo – Directrices* (Norma ISO N. 31000). https://www.iso.org/standard/65556.html.

Organización Internacional de Normalización. (2019). *Seguridad y resiliencia – Sistemas de gestión de continuidad del negocio – Requisitos* (Norma ISO N. 22301). https://www.iso.org/standard/75106.html.

Organización Internacional de Normalización. (2021). *Seguridad de la información, ciberseguridad y protección de la privacidad – Seguridad de la información para las relaciones con los proveedores* (Norma ISO/IEC N. 27036). https://www.iso.org/standard/77402.html.

Organización Internacional de Normalización. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad – Recomendaciones para la gestión de riesgos de seguridad de la información* (Norma ISO/IEC N. 27005). https://www.iso.org/standard/83724.html.

Reglamento de la Unión Europea 679 de 2016 [Parlamento Europeo]. Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). 27 de abril de 2016.

CONTINUAR

Lección 4 de 4

Descarga en PDF

PDF

Gestión de riesgos, continuidad y terceros.pdf

463.4 KB