1 Introducción

En la actual era digital, los activos de información se han convertido en uno de los recursos más estratégicos y valiosos para las organizaciones, independientemente de su tamaño o sector. Estos activos no sólo comprenden datos digitales, sino también el conocimiento, los procesos y los sistemas que permiten su utilización, procesamiento y resguardo. La correcta administración de estos activos no solo asegura la continuidad operativa, sino que también protege el prestigio institucional, el cumplimiento normativo y la competitividad.

En este contexto, las organizaciones enfrentan un entorno caracterizado por crecientes amenazas tanto internas como externas, así como por una superficie de ataque ampliada por la incorporación de nuevas tecnologías. Las vulnerabilidades técnicas, humanas y procedimentales pueden derivar en incidentes que comprometan la confidencialidad, integridad o disponibilidad de la información.

Frente a ello, se vuelve indispensable establecer una estrategia integral orientada a preservar el valor de los activos de información. Esta estrategia debe contemplar la evaluación constante del riesgo, la adopción de mecanismos de protección, la capacitación del personal, la definición de políticas claras y la colaboración entre todos los actores involucrados. Este trabajo analiza los componentes críticos de dicha estrategia y propone un marco estructurado para su aplicación.

2 El valor de los activos de información

Los activos de información son todos aquellos elementos tangibles e intangibles que permiten a una organización generar, almacenar, procesar y utilizar información para cumplir con sus objetivos institucionales y operativos. Entre ellos se encuentran bases de datos, documentos digitales, sistemas informáticos, algoritmos, registros en papel, así como el conocimiento tácito de los empleados. Su valor se puede comprender desde diferentes perspectivas: económica, estratégica, legal y reputacional.

Desde una perspectiva económica, la pérdida o alteración de un activo de información puede derivar en pérdidas financieras directas (fraudes, multas, paralización operativa). En el plano estratégico, estos activos permiten desarrollar ventajas competitivas y mejorar procesos. Legalmente, el incumplimiento de normas de resguardo de datos puede acarrear sanciones severas, como ocurre con

el RGPD en Europa o la Ley 25.326 en Argentina. En términos de reputación, una violación de seguridad puede afectar la confianza de clientes, accionistas y socios estratégicos.

Para preservar estos valores, se utilizan criterios como la confidencialidad (quién puede acceder), la integridad (si la información es exacta y no ha sido alterada) y la disponibilidad (que esté accesible cuando se necesita). A través de estos tres pilares se evalúa la criticidad de cada activo y se definen niveles de protección.

3 Tipología de amenazas

3.1 Amenazas internas y externas

Las amenazas que afectan a los activos de información pueden clasificarse según su origen en internas y externas. Las amenazas internas provienen de individuos que tienen acceso autorizado a los sistemas, como empleados, contratistas, socios o exempleados. Estas amenazas pueden manifestarse en forma de abuso de privilegios, negligencia, sabotaje, robo de información o manipulación de registros. Incluso el error humano involuntario, como el envío de un correo con datos sensibles a un destinatario incorrecto, representa un riesgo considerable.

Las amenazas externas, en cambio, provienen de actores ajenos a la organización y suelen tener como objetivo obtener acceso no autorizado, provocar daños o extorsionar. Incluyen ataques de malware, ransomware, phishing, denegación de servicios distribuidos (DDoS), espionaje industrial y campañas de ingeniería social. Los ciberdelincuentes, hacktivistas, competidores y grupos patrocinados por estados son parte del conjunto de actores externos.

3.2 Amenazas voluntarias e involuntarias

Otro criterio para clasificar las amenazas es su intencionalidad. Las amenazas voluntarias son aquellas que se ejecutan con una intención maliciosa deliberada. Incluyen conductas como el fraude interno, la filtración de documentos sensibles, el sabotaje tecnológico o la instalación de software espía. Estas amenazas suelen ser más complejas de detectar, ya que muchas veces provienen de usuarios con permisos válidos.

Por otro lado, las amenazas involuntarias o provocadas sin intención surgen del desconocimiento, la negligencia o circunstancias ajenas al control humano. Por ejemplo, errores de configuración en un servidor, dejar dispositivos sin protección, fallas eléctricas, desastres naturales o incluso pandemias, pueden provocar brechas de seguridad o interrupciones críticas en los sistemas.

Este doble enfoque de análisis (interno/externo, voluntario/involuntario) permite a las organizaciones tener una visión más clara y amplia del espectro de riesgos al que se enfrentan, facilitando la priorización de medidas y la asignación de recursos de forma estratégica.

4 Vulnerabilidades en los sistemas de información

Las vulnerabilidades son debilidades inherentes a los sistemas, procesos o comportamientos humanos que pueden ser explotadas por amenazas para comprometer los activos de información. Estas debilidades pueden clasificarse en técnicas, organizacionales y humanas, y su existencia es un componente crítico en la gestión de la seguridad, dado que representan puntos de entrada para posibles incidentes.

Entre las vulnerabilidades técnicas más frecuentes se encuentran las configuraciones inseguras de software, sistemas operativos desactualizados, errores de programación (como desbordamientos de búfer o inyecciones SQL), y fallas en la autenticación o autorización de usuarios. Estas vulnerabilidades pueden encontrarse tanto en aplicaciones comerciales como en desarrollos propios, y su identificación requiere un proceso constante de auditoría y análisis.

Las vulnerabilidades organizacionales están asociadas a la falta de políticas claras, ausencia de controles internos, estructuras desactualizadas de acceso a la información, o procesos inadecuados de respaldo y recuperación. También pueden darse por la inexistencia de un plan de continuidad operativa o la subestimación del área de seguridad dentro del gobierno corporativo.

Finalmente, las vulnerabilidades humanas constituyen uno de los elementos más críticos. La falta de formación, la negligencia, el uso de contraseñas débiles, la reutilización de claves en múltiples servicios y la caída ante técnicas de ingeniería social, como el phishing, abren importantes brechas que los atacantes suelen explotar con mayor facilidad que los fallos técnicos.

El reconocimiento, categorización y priorización de estas vulnerabilidades es esencial para establecer un plan de seguridad efectivo. No basta con identificar una vulnerabilidad; se deben estimar sus impactos potenciales, la probabilidad de explotación y las posibles consecuencias para los activos afectados.

5 Mecanismos de seguridad de la información

Frente a las amenazas y vulnerabilidades descritas, las organizaciones deben implementar una serie de mecanismos de seguridad que garanticen la protección de los activos de información en todas sus dimensiones. Estos mecanismos deben estar alineados a los principios de confidencialidad, integridad y disponibilidad, y deben ser proporcionales al nivel de riesgo.

Entre los mecanismos más relevantes se encuentran:

- Controles de acceso: Establecimiento de reglas para limitar quién puede acceder a qué información y bajo qué condiciones. El uso de modelos como el control de acceso basado en roles (RBAC) o el control basado en atributos (ABAC) permite granularidad y adaptabilidad.
- Autenticación multifactor (MFA): Refuerza la identificación del usuario combinando al menos dos métodos distintos (algo que sabe, algo que tiene o algo que es).
- Cifrado de datos: Tanto en tránsito como en reposo, para proteger la confidencialidad frente a accesos no autorizados.
- Firewalls y sistemas de detección/previsión de intrusos (IDS/IPS): Herramientas de monitoreo y bloqueo de tráfico malicioso o no autorizado.
- Sistemas de respaldo (backups): Copias de seguridad periódicas, con almacenamiento en sitios seguros y pruebas de restauración, para garantizar la recuperación ante incidentes.
- Actualización y parcheo de sistemas: Eliminación de vulnerabilidades conocidas mediante políticas estrictas de mantenimiento.
- Registro y auditoría de eventos (logging): Recolección de evidencia digital para monitorear comportamientos sospechosos y facilitar la respuesta ante incidentes.
- Planes de gestión de incidentes y continuidad operativa: Establecimiento de protocolos definidos para actuar ante una brecha, reducir su impacto y asegurar el retorno a la normalidad.

La combinación de estos mecanismos, en un enfoque defense-in-depth (defensa en profundidad), asegura que no exista un único punto de falla, y permite a la organización resistir, responder y recuperarse de los incidentes.

6 Gestión de riesgos tecnológicos

La gestión del riesgo es el pilar central de toda estrategia de seguridad de la información. Consiste en identificar, evaluar y tratar los riesgos derivados del uso de tecnologías dentro de la organización, con el objetivo de minimizar su probabilidad de ocurrencia o su impacto.

Este proceso generalmente incluye cuatro etapas principales:

- Identificación de activos, amenazas y vulnerabilidades: Se establece qué se desea proteger, frente a qué amenazas, y qué debilidades podrían ser explotadas.
- Análisis y evaluación del riesgo: Se estima la probabilidad de ocurrencia de un incidente y las consecuencias que tendría sobre los activos, utilizando matrices de impacto y riesgo.
- Tratamiento del riesgo: Las opciones incluyen aceptar el riesgo, mitigarlo (implementando controles), transferirlo (por ejemplo, mediante seguros o contratos) o evitarlo (no ejecutar ciertas actividades).
- Monitoreo y revisión continua: El riesgo es dinámico; por lo tanto, debe ser revaluado periódicamente en función de cambios tecnológicos, regulatorios y organizacionales.

Existen metodologías ampliamente reconocidas para guiar este proceso, como ISO/IEC 27005, ISO 31000, NIST Risk Management Framework y OCTAVE. Estas metodologías proponen estructuras sistemáticas para gestionar el riesgo dentro del marco más amplio de la gobernanza corporativa.

Además, se deben definir controles preventivos (que buscan evitar el incidente), controles detectivos (que lo identifican oportunamente), y controles correctivos (que lo mitigan o eliminan). La adecuada combinación de estos controles permite una gestión eficiente del riesgo residual.

Incorporar la gestión de riesgos en todas las capas de la organización, desde la alta dirección hasta los niveles operativos, es fundamental para una seguridad efectiva, orientada a la resiliencia y al cumplimiento normativo.

7 Cultura organizacional, concientización y capacitación

El componente humano representa uno de los eslabones más vulnerables en la cadena de seguridad de la información. Por ello, establecer una cultura organizacional orientada a la seguridad es tan relevante como implementar herramientas tecnológicas. La concientización y la capacitación sistemática de los colaboradores son acciones clave para reducir riesgos y fomentar una conducta responsable frente a los activos de información.

Una cultura sólida en seguridad se construye desde la alta dirección, promoviendo valores como la responsabilidad, la transparencia, la prevención y el cumplimiento normativo. Esta cultura se consolida cuando la seguridad se integra en los procesos diarios de trabajo y no es vista como una carga externa, sino como una práctica necesaria y beneficiosa.

Los programas de concientización deben estar dirigidos a todos los niveles jerárquicos y contemplar diversas modalidades: capacitaciones presenciales, módulos interactivos en línea, campañas visuales, simulaciones de ataques (por ejemplo, phishing controlado), y la comunicación de incidentes reales para reforzar el aprendizaje. Además, deben actualizarse regularmente para reflejar nuevos escenarios de riesgo.

En paralelo, la formación técnica específica para roles críticos (como administradores de sistemas, desarrolladores, auditores y personal de soporte) debe asegurar que cada actor conozca sus responsabilidades y maneje buenas prácticas alineadas con los estándares del sector.

Una organización que invierte en educación en seguridad no solo protege sus activos, sino que también desarrolla capital humano consciente, proactivo y resiliente frente a las amenazas.

8 Seguridad en la selección y gestión del personal

La seguridad de los activos de información comienza incluso antes de que una persona ingrese a la organización. El proceso de selección y contratación debe incorporar criterios de seguridad desde el primer momento, asegurando que quienes accedan a información sensible lo hagan con integridad, confiabilidad y responsabilidad.

En esta línea, se recomienda implementar:

- Verificación de antecedentes personales y laborales, respetando el marco legal vigente.
- Entrevistas estructuradas que incluyan evaluaciones sobre ética profesional, cumplimiento de normas y manejo de información confidencial.
- Cláusulas contractuales específicas que incluyan deberes de confidencialidad, cumplimiento de políticas internas y consecuencias ante el uso indebido de recursos informáticos.

Durante la relación laboral, es fundamental aplicar el principio de privilegio mínimo: cada usuario debe contar con los accesos necesarios y suficientes para su función, evitando otorgar permisos innecesarios que puedan representar un riesgo.

Asimismo, deben establecerse procesos para la gestión de cambios en los roles, ascensos o traslados, revisando y ajustando los privilegios asignados. Al momento de la desvinculación del empleado, debe aplicarse un procedimiento estandarizado para revocar accesos, recuperar dispositivos y recordarle al colaborador las obligaciones de confidencialidad que subsisten incluso luego del vínculo laboral.

El personal también debe ser monitoreado desde una perspectiva ética y técnica, con controles proporcionales y respetuosos de la privacidad, pero orientados a la prevención de conductas que pongan en riesgo los activos de la organización.

9 Políticas de seguridad y marco normativo

Las políticas de seguridad de la información constituyen el marco normativo interno que guía el comportamiento de los colaboradores, los procedimientos técnicos y los criterios de cumplimiento de la organización. Estas políticas deben ser claras, accesibles, actualizadas y aprobadas por la alta dirección, lo que refleja su importancia estratégica.

Una política bien estructurada incluye:

- Clasificación de la información y criterios de acceso.
- Uso aceptable de los recursos tecnológicos.
- Gestión de incidentes de seguridad.

- Política de backups y recuperación.
- Gestión de accesos y contraseñas.
- Seguridad en la contratación de terceros.
- Uso de dispositivos móviles y trabajo remoto.
- Conservación y destrucción segura de la información.

Estas políticas deben ser difundidas mediante campañas internas, incluidas en los manuales de bienvenida y firmadas por todos los empleados. Asimismo, deben estar alineadas con las normas internacionales reconocidas como la ISO/IEC 27001, que establece requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información.

Desde el punto de vista externo, las organizaciones deben cumplir con un conjunto de regulaciones legales aplicables según su jurisdicción y sector. Ejemplos clave incluyen:

- Ley 25.326 de Protección de Datos Personales (Argentina).
- Reglamento General de Protección de Datos (RGPD/GDPR) en la Unión Europea.
- Ley Sarbanes-Oxley (SOX) para empresas que cotizan en bolsa en EE.UU.
- Ley HIPAA en el sector salud estadounidense.
- Estándar PCI-DSS para la industria de tarjetas de pago.

Cumplir con estas normativas no solo evita sanciones legales, sino que también posiciona a la organización como un actor confiable frente a clientes, socios y organismos de control.

10 Estrategias de seguridad colaborativa

La seguridad de la información no puede depender exclusivamente del área de sistemas o de tecnología: debe concebirse como una responsabilidad compartida que involucra a todos los niveles y sectores de la organización. En este sentido, las estrategias de seguridad colaborativa proponen integrar a múltiples actores —internos y externos— en el diseño, implementación y mejora continua de las políticas de protección de los activos de información.

Desde adentro de la organización, es indispensable articular esfuerzos entre:

- Dirección general, que debe proveer liderazgo, recursos y legitimidad política a las iniciativas de seguridad.
- Área de tecnología, responsable de implementar las soluciones técnicas y operativas.
- Recursos humanos, como actor clave en los procesos de concientización, capacitación y selección de personal.
- Departamento legal, encargado de asegurar el cumplimiento de las normativas y el tratamiento adecuado de datos personales.
- Auditoría y control interno, cuya función es evaluar el cumplimiento y la eficacia de los mecanismos implementados.

Desde afuera, las organizaciones también deben considerar la gestión de terceros, como proveedores, consultores, contratistas y aliados estratégicos. La relación con estos actores requiere acuerdos contractuales que establezcan niveles de seguridad esperados, así como procesos de evaluación, monitoreo y auditoría.

Las buenas prácticas de seguridad colaborativa incluyen la creación de comités de seguridad de la información interdisciplinarios, espacios de reporte de incidentes abiertos y sin represalias, evaluaciones conjuntas de riesgo, y sistemas de comunicación internos donde cada área pueda canalizar dudas o propuestas de mejora.

Fomentar la participación activa de todos los sectores favorece no sólo la eficacia técnica de la estrategia, sino también la apropiación institucional de una cultura de seguridad duradera y sostenible.

11 Estrategia integral de seguridad organizacional

Una estrategia de seguridad organizacional debe ser holística, estructurada y dinámica, es decir, abarcar todos los componentes críticos de la organización, estar basada en principios de gobernanza y ajustarse permanentemente a un entorno cambiante.

Los principales pilares de esta estrategia incluyen:

- Gobierno de la seguridad: Definición de responsabilidades, roles y autoridades. Creación de un comité de seguridad de la información con representación transversal.
- Evaluación y gestión del riesgo: Identificación periódica de amenazas, vulnerabilidades e impactos; determinación de controles y aceptación del riesgo residual.
- Desarrollo de políticas y normativas: Conjunto de documentos que regulan el comportamiento de las personas, los procesos y la tecnología.
- Capacitación y concientización continua: Formación de usuarios como primera línea de defensa frente a amenazas comunes.
- Protección tecnológica: Implementación de mecanismos técnicos (cifrado, firewalls, autenticación) y sistemas de monitoreo continuo.
- Gestión de incidentes: Diseño de protocolos que incluyan identificación, contención, remediación, recuperación y documentación.
- Continuidad operativa y recuperación ante desastres: Asegurar que la organización pueda seguir operando, o restablecer sus funciones críticas, ante eventos disruptivos.
- Mejora continua: Aplicación del ciclo PDCA (Plan-Do-Check-Act) para ajustar políticas, controles y procesos en función de auditorías, incidentes o cambios del entorno.

Una estrategia integral debe, además, alinearse con los objetivos de negocio, priorizando la protección de los activos más críticos y asegurando que las inversiones en seguridad generen valor para la organización. No se trata de eliminar todos los riesgos, lo cual es imposible, sino de gestionar los riesgos aceptables de manera efectiva y sostenible.

12 Conclusiones

La protección del valor de los activos de información en las organizaciones contemporáneas exige una estrategia amplia, proactiva y alineada con los objetivos institucionales. En un entorno caracterizado por la hiperconectividad, la creciente sofisticación de las amenazas y el marco normativo cada vez más exigente, ya no es suficiente con contar con herramientas tecnológicas

aisladas: es necesario articular personas, procesos y tecnologías dentro de una visión integral de la seguridad.

A lo largo del presente trabajo se han identificado y desarrollado los principales componentes de una estrategia efectiva: el análisis de amenazas y vulnerabilidades, la implementación de mecanismos técnicos de protección, la gestión de riesgos, la capacitación continua del personal, la formulación de políticas claras y el establecimiento de una cultura de seguridad compartida.

Asimismo, se ha enfatizado la necesidad de una gestión colaborativa, en la que todos los sectores de la organización participen en la construcción y mantenimiento de un entorno seguro. La seguridad no debe ser vista como un gasto, sino como una inversión estratégica que preserva la continuidad operativa, la reputación institucional y la confianza de los clientes.

Finalmente, se reafirma que la seguridad de la información no es un estado, sino un proceso dinámico de mejora continua, que debe adaptarse a los cambios tecnológicos, organizacionales y sociales. Solo aquellas organizaciones que asuman esta visión como parte de su cultura corporativa estarán preparadas para enfrentar los desafíos del presente y del futuro.

13 Guía de Implementación: Estrategia de Seguridad de la Información en una Organización

- Rubro: Servicios tecnológicos y desarrollo de software.
- Tamaño: Mediana empresa (120 empleados).
- Infraestructura crítica: Sistemas de gestión ERP, servidores en la nube, bases de datos de clientes, contratos confidenciales.

13.1 Fase 1 – Evaluación inicial y diagnóstico

- Conformación del Comité de Seguridad de la Información, integrado por representantes de IT, RR.HH., Legal, Operaciones y Alta Dirección.
- Inventario de activos de información, clasificándolos según su criticidad (datos personales, financieros, propiedad intelectual, etc.).

- Evaluación de amenazas y vulnerabilidades mediante entrevistas, análisis de logs, escaneo de infraestructura y auditoría documental.
- Análisis de cumplimiento normativo, considerando ISO 27001, Ley 25.326, y obligaciones contractuales con clientes internacionales.

13.2 Fase 2 – Planificación estratégica

Definición de objetivos de seguridad alineados al negocio, tales como:

- Evitar fugas de datos sensibles.
- Garantizar continuidad ante cortes de servicio.
- Cumplir con requerimientos regulatorios y de clientes.
- Desarrollo del Mapa de Riesgos Tecnológicos, utilizando matriz de impacto-probabilidad.
- Diseño del Plan de Seguridad de la Información, que incluya políticas de acceso, cifrado, backup, gestión de incidentes, y relaciones con terceros.

13.3 Fase 3 – Implementación técnica y organizacional

Despliegue de controles técnicos prioritarios:

- Autenticación multifactor en todas las cuentas críticas.
- Segmentación de red y firewall actualizado.
- Cifrado de discos duros y backup automático off-site.
- SIEM básico (sistema de monitoreo de eventos de seguridad).

Implementación de políticas organizacionales:

- Manual de Seguridad Informática.
- Código de Conducta Digital.
- Protocolo de respuesta ante incidentes.

- Actualización de contratos con proveedores incorporando cláusulas de confidencialidad, gestión de datos y notificación de incidentes.

Fase 4 – Capacitación y cultura de seguridad

Campañas de concientización para empleados, incluyendo:

- Curso de phishing y redes sociales.
- Boletines mensuales de seguridad.
- Ejercicios prácticos de simulación de incidentes.
- Capacitación especializada para administradores y desarrolladores sobre hardening de sistemas, OWASP Top 10, y gestión segura del ciclo de vida del software.
- Evaluación anual de madurez cultural en seguridad, mediante encuestas internas y métricas de comportamiento (e.g., respuesta a simulacros).

13.4 Fase 5 – Monitoreo, control y mejora continua

- Revisión trimestral del cumplimiento de políticas mediante controles internos.
- Auditorías anuales externas de seguridad y cumplimiento normativo.
- Análisis post mortem de incidentes para ajustar procedimientos y controles.
- Actualización del mapa de riesgos y plan estratégico al menos una vez por año.

Resultados esperados

- Reducción de incidentes de seguridad en un 60% durante el primer año.
- Mayor confianza de los clientes estratégicos y certificaciones de cumplimiento.
- Aumento en la resiliencia organizacional ante contingencias tecnológicas.
- Instalación de una cultura organizacional sólida y comprometida con la protección de los activos de información.