Seguridad de la información en las Tecnologías de la Información

1 Introducción: la seguridad (security) en las Tecnologías de la Información

1.1 Concepto central

En el campo de la administración y de las Tecnologías de la Información, la palabra "seguridad" puede generar una confusión inicial porque en inglés existen dos términos distintos que en español suelen traducirse de forma parecida: **safety** y **security**.

Esta diferencia puede ordenarse del siguiente modo. **Safety** se vincula con riesgos conocidos, generalmente no maliciosos, asociados a accidentes, fallas operativas, procesos productivos, salud, infraestructura o continuidad física. **Security**, en cambio, se vincula con amenazas intencionales, dinámicas y muchas veces originadas fuera de la organización. En términos de TI, security se relaciona con ciberseguridad, protección de datos, accesos indebidos, fraude, malware, ransomware, phishing, espionaje, sabotaje, abuso de privilegios y ataques contra sistemas de información.

La diferencia principal es la **intencionalidad**. En safety, el riesgo suele provenir de una falla, un accidente, un error o una condición peligrosa no buscada deliberadamente. En security, el riesgo suele provenir de un actor que intenta causar daño, obtener beneficio indebido, robar información, alterar sistemas o interrumpir servicios.

Desde la administración de empresas, esta diferencia es relevante porque cambia la forma de evaluar, prevenir y responder. No se administra igual el riesgo de que un servidor falle por temperatura excesiva que el riesgo de que un atacante robe credenciales para ingresar a un sistema de pagos. Ambos casos son importantes, pero la lógica de análisis no es la misma.

1.2 Comparación entre safety y security

Safety y security pueden compararse a partir de cinco criterios: naturaleza del riesgo, tipo de intención, datos históricos, tipo de evaluación del riesgo y posibilidad de mitigación.

Criterio	Safety	Security
Naturaleza del riesgo	Riesgos relacionados con producción, operación o beneficio, generalmente conocidos	Amenazas humanas, estratégicas, dinámicas y muchas veces originadas fuera de la organización
Tipo de intención	Intención no maliciosa	Intención deliberada y maliciosa
Datos históricos	Los datos históricos suelen servir para predecir tendencias	Los datos históricos pueden ser problemáticos y no siempre predicen el futuro
Evaluación del riesgo	Se utilizan con frecuencia probabilidades y frecuencias cuantitativas	Se utilizan con frecuencia análisis cualitativos y opinión experta
Mitigación	La organización suele conocer escenarios posibles y medidas aplicables	Las amenazas y medidas pueden ser más inciertas, simbólicas o difíciles de anticipar

Esto permite comprender que la seguridad en sentido de **security** no puede tratarse como una simple administración de incidentes repetitivos. En ciberseguridad, el riesgo cambia porque los atacantes aprenden, se adaptan, ocultan sus rastros, explotan nuevas vulnerabilidades y modifican sus técnicas según las defensas de la organización.

1.3 Seguridad como protección frente a amenazas intencionales

En Tecnologías de la Información, la seguridad debe entenderse como el conjunto de políticas, controles, tecnologías, procesos y responsabilidades destinadas a proteger sistemas, datos, usuarios, redes, aplicaciones e infraestructura frente a amenazas intencionales.

Esto incluye proteger:

Activo protegido	Riesgo de security
Datos de clientes	Robo, filtración, uso indebido o venta no autorizada
Sistemas administrativos	Acceso ilegítimo, alteración de registros o fraude
Correo electrónico	Phishing, suplantación, malware o robo de credenciales
Infraestructura tecnológica	Intrusión, sabotaje, explotación de vulnerabilidades
Aplicaciones web	Ataques, inyección de código, abuso de sesiones
Identidades digitales	Uso indebido de cuentas, contraseñas o tokens
Proveedores tecnológicos	Accesos externos no controlados o fallas de cadena de suministro
Respaldos	Borrado, cifrado malicioso o manipulación

La seguridad no se limita a instalar herramientas. Un antivirus, un firewall o una contraseña son controles puntuales. La security requiere una arquitectura de gestión:

identificación de activos, análisis de amenazas, políticas de acceso, monitoreo, respuesta a incidentes, capacitación, gobierno de proveedores y auditoría.

1.4 Diferencia entre accidente, error y ataque

En security existe intencionalidad maliciosa. Esto obliga a distinguir tres situaciones: accidente, error y ataque.

Situación	Característica	Ejemplo en TI	Tipo de enfoque
Accidente	Ocurre sin intención dañina	Corte eléctrico que apaga servidores	Continuidad, redundancia y recuperación
Error	Surge por acción humana no maliciosa	Un usuario envía una base de clientes al destinatario equivocado	Capacitación, validación y controles preventivos
Ataque	Existe intención de causar daño u obtener beneficio indebido	Un atacante roba credenciales mediante phishing	Ciberseguridad, detección, respuesta y evidencia

Esta distinción es central para la administración. Si se interpreta un ataque como si fuera solo una falla operativa, la organización puede responder de manera insuficiente. Por ejemplo, si se detectan accesos inusuales a una base de datos y se los trata como un error de sistema, se puede perder tiempo crítico para contener una intrusión.

1.5 Naturaleza dinámica de las amenazas de seguridad

En safety, muchos riesgos son relativamente estables. Si una máquina tiene una pieza defectuosa, el riesgo puede analizarse con datos técnicos, frecuencia de fallas, historial de mantenimiento y condiciones de operación. En security, el escenario es distinto porque existe un actor que decide, observa, aprende y adapta su conducta.

En ciberseguridad, el atacante puede cambiar de técnica si la organización mejora sus defensas. Si se bloquean adjuntos peligrosos, puede usar enlaces. Si se implementa autenticación multifactor, puede intentar engañar al usuario para aprobar una notificación. Si se segmenta la red, puede buscar credenciales privilegiadas. Si se fortalecen sistemas internos, puede atacar a un proveedor.

Por eso, la seguridad en TI debe verse como una función dinámica. No alcanza con diseñar controles una vez y dejarlos sin revisión. La organización debe monitorear, actualizar, probar, corregir y aprender de incidentes propios y ajenos.

Amenaza	Por qué es dinámica
Phishing	Cambia el contenido del engaño según contexto, urgencia o autoridad simulada
Ransomware	Evoluciona hacia doble extorsión, robo de datos y presión reputacional
Ataques a proveedores	Aprovechan terceros con accesos legítimos
Robo de credenciales	Usa filtraciones previas, ingeniería social y malware
Abuso interno	Puede ser realizado por usuarios con permisos válidos
Ataques a la nube	Explotan errores de configuración, claves expuestas o permisos excesivos

1.6 Datos históricos: utilidad y límites

En safety, los datos históricos suelen ser aplicables para predecir tendencias futuras. En security, en cambio, los datos históricos son más problemáticos.

Esto no significa que los datos históricos no sirvan. Sirven para conocer incidentes pasados, tendencias, vulnerabilidades recurrentes, tiempos de respuesta, cantidad de ataques bloqueados, usuarios afectados y sistemas más expuestos. Pero no siempre permiten anticipar ataques futuros, porque las amenazas cambian.

Una organización puede haber tenido pocos incidentes durante años y aun así estar expuesta a un ataque grave si aparece una nueva vulnerabilidad, si un proveedor es comprometido o si un usuario entrega credenciales. También puede tener muchos intentos bloqueados y no sufrir incidentes porque los controles funcionan.

La administración debe interpretar los datos con cuidado.

Dato histórico	Utilidad	Límite
Cantidad de intentos de phishing	Permite medir exposición de usuarios	No predice exactamente el próximo engaño
Incidentes de malware del año anterior	Permite identificar áreas vulnerables	Puede no reflejar nuevas variantes
Tiempo medio de respuesta	Permite medir madurez operativa	No garantiza capacidad ante crisis mayor
Vulnerabilidades corregidas	Permite medir gestión técnica	No asegura que no existan fallas no detectadas
Accesos no autorizados previos	Permite mejorar controles	No contempla cambios en tácticas del atacante

Por eso, en security se combinan datos, monitoreo, inteligencia de amenazas, experiencia de especialistas, pruebas de seguridad y evaluación de escenarios.

1.7 Evaluación del riesgo en security

En safety se utilizan con frecuencia evaluaciones cuantitativas basadas en probabilidades y frecuencias. En security, en cambio, suele ser necesario recurrir a evaluación cualitativa, opinión experta y análisis de probabilidad estimada.

En TI, muchos riesgos de seguridad no pueden medirse con precisión matemática absoluta. No siempre se sabe cuántos atacantes intentarán ingresar, qué técnica usarán, qué vulnerabilidad será explotada o cuándo ocurrirá el incidente. Por eso, la evaluación de security combina criterios cuantitativos y cualitativos.

Criterio de evaluación	Aplicación en security
Probabilidad estimada	Qué tan posible es que ocurra el ataque
Impacto	Qué daño generaría sobre datos, sistemas, finanzas, reputación o cumplimiento
Exposición	Qué tan accesible está el activo para un atacante
Vulnerabilidad	Qué debilidad puede ser explotada
Capacidad de detección	Qué tan rápido se detectaría el evento
Capacidad de respuesta	Qué tan rápido se podría contener
Valor del activo	Qué importancia tiene el dato o sistema afectado
Motivación del atacante	Qué interés puede tener en atacar a la organización

Una evaluación madura no se limita a preguntar si “ya ocurrió antes”. Debe preguntar qué podría ocurrir, quién podría intentarlo, qué activos están expuestos, qué controles existen y qué impacto tendría la materialización del riesgo.

1.8 Security en sistemas de información

En sistemas de información, la security debe proteger la confidencialidad, integridad y disponibilidad de los datos y servicios.

Principio	Qué protege	Ejemplo
Confidencialidad	Que solo accedan personas autorizadas	Evitar que un usuario sin permiso consulte legajos salariales
Integridad	Que los datos no sean alterados indebidamente	Evitar que se modifique una cuenta bancaria de proveedor sin aprobación
Disponibilidad	Que sistemas y datos estén accesibles cuando se necesitan	Evitar que un ataque de ransomware paralice facturación

Estos tres principios suelen conocerse como la tríada CIA (Confidentiality, Integrity and Availability, confidencialidad, integridad y disponibilidad). En security, los tres pueden verse afectados por acciones maliciosas.

Un atacante puede vulnerar la confidencialidad robando datos. Puede afectar la integridad modificando registros. Puede afectar la disponibilidad interrumpiendo servicios. En algunos incidentes, los tres principios se ven comprometidos al mismo tiempo.

Ejemplo: en un ataque de ransomware, los datos pueden ser robados, cifrados y amenazados con publicación. Allí se afecta la confidencialidad por la posible filtración, la disponibilidad por el bloqueo de acceso y la integridad si los archivos fueron modificados o dañados.

1.9 Seguridad como problema estratégico

La security es un riesgo estratégico y humano. La seguridad no debe entenderse solo como una función técnica. Es una cuestión estratégica porque afecta objetivos de negocio,

continuidad, confianza, reputación, cumplimiento legal y relación con clientes y proveedores.

Un incidente de seguridad puede producir:

Impacto	Ejemplo
Económico	Costos de recuperación, pérdida de ventas o multas
Operativo	Interrupción de sistemas críticos
Legal	Incumplimiento de normas de protección de datos
Reputacional	Pérdida de confianza de clientes
Contractual	Incumplimiento de acuerdos de nivel de servicio
Organizacional	Pérdida de productividad y crisis interna
Competitivo	Filtración de información estratégica

La seguridad exige decisiones de dirección. Debe definirse qué activos son críticos, qué nivel de riesgo se acepta, qué presupuesto se asigna, qué controles son obligatorios, qué proveedores acceden a información sensible y cómo se reportan incidentes.

En este sentido, security es parte del gobierno de TI y del gobierno organizacional. No puede delegarse completamente en técnicos. El área de TI implementa controles, pero la dirección debe definir prioridades, tolerancia al riesgo y responsabilidades.

1.10 Ejemplos aplicados a Tecnologías de la Información

1.10.1 Caso 1: phishing a usuarios administrativos

Un empleado recibe un correo que simula provenir del área de sistemas. El mensaje solicita validar la contraseña para evitar el bloqueo de la cuenta. El usuario ingresa sus credenciales en un sitio falso. El atacante utiliza esos datos para acceder al correo y buscar información sobre pagos.

Elemento	Análisis
Tipo de riesgo	Security
Intención	Maliciosa
Actor	Externo
Activo afectado	Credenciales y correo corporativo
Impacto posible	Fraude, robo de información o acceso a otros sistemas
Control preventivo	Capacitación, MFA y filtros antiphishing
Control detectivo	Alertas por inicio de sesión anómalo
Control correctivo	Revocación de sesiones y cambio de credenciales

Este caso muestra que el riesgo no se origina en una falla accidental, sino en un engaño deliberado.

1.10.2 Caso 2: proveedor tecnológico comprometido

Una organización contrata a un proveedor para mantener una aplicación interna. El proveedor tiene acceso remoto permanente. Su cuenta no usa autenticación multifactor. Un atacante compromete al proveedor e ingresa a la red de la organización usando credenciales válidas.

Elemento	Análisis
Tipo de riesgo	Security
Intención	Maliciosa
Actor	Externo a través de tercero

Elemento	Análisis
Activo afectado	Red interna y aplicación mantenida
Impacto posible	Intrusión, robo de datos o sabotaje
Control preventivo	Accesos mínimos, MFA, VPN controlada y ventanas de acceso
Control detectivo	Monitoreo de accesos de terceros
Control contractual	Cláusulas de seguridad y auditoría

Este caso muestra que security también incluye la cadena de suministro tecnológica.

1.10.3 Caso 3: ransomware sobre servidor de archivos

Un usuario abre un archivo malicioso. El malware se ejecuta, cifra carpetas compartidas y bloquea documentos críticos. Luego aparece una nota de extorsión solicitando pago para recuperar el acceso.

Elemento	Análisis
Tipo de riesgo	Security
Intención	Maliciosa
Activo afectado	Documentos, carpetas compartidas y continuidad operativa
Impacto posible	Interrupción, pérdida de datos, extorsión y daño reputacional
Control preventivo	EDR, capacitación, restricción de macros y parches
Control recuperatorio	Backups inmutables y plan de recuperación

Elemento	Análisis
Control de respuesta	Aislamiento de equipos y activación del plan de incidentes

El caso muestra que la seguridad no se agota en evitar el ataque. También requiere detectar, contener y recuperar.

1.11 Diferencia práctica entre safety y security en TI

Aunque ambos conceptos se vinculan con protección, en la gestión tecnológica conviene distinguirlos.

Situación	Safety	Security
Falla de aire acondicionado en sala de servidores	Riesgo operativo o ambiental	Puede afectar disponibilidad, pero no surge de intención maliciosa
Ataque que apaga equipos críticos	No es safety puro	Es security porque existe acción intencional
Usuario que borra un archivo por error	Error no malicioso	Puede generar incidente, pero no ataque
Usuario que borra datos para ocultar fraude	No es accidente	Es security por intención indebida
Corte eléctrico general	Riesgo de continuidad	Puede requerir planes de respaldo
Sabotaje sobre suministro eléctrico	Amenaza intencional	Security física y tecnológica

En la práctica, una organización necesita gestionar ambas dimensiones. Sin embargo, cuando se habla de seguridad de la información, ciberseguridad o protección de sistemas, el foco principal está en **security**.

1.12 Mitigación en security: por qué es más compleja

En safety, la organización suele conocer mejor los escenarios posibles y las medidas aplicables. En security, las amenazas y medidas pueden ser más inciertas.

Esto se debe a varios motivos:

- Los atacantes cambian de técnica.
- Las vulnerabilidades aparecen en sistemas nuevos y existentes.
- Los usuarios pueden ser engañados.
- Los proveedores también pueden ser atacados.
- Las herramientas de seguridad pueden estar mal configuradas.
- El riesgo puede aparecer en activos no inventariados.
- Las medidas pueden ser insuficientes si no se monitorean.
- Algunas defensas generan fricción operativa.
- La organización puede creer que está protegida solo porque compró herramientas.
- Los incidentes pueden permanecer ocultos durante largo tiempo.

Mitigar security exige combinar controles.

Tipo de control	Ejemplo
Preventivo	MFA, segmentación, hardening, capacitación

Tipo de control	Ejemplo
Detectivo	SIEM, EDR, monitoreo de logs, alertas
Correctivo	Revocación de accesos, cierre de vulnerabilidades
Recuperatorio	Backups, restauración, continuidad del negocio
Administrativo	Políticas, auditoría, gestión de proveedores
Legal y contractual	Cláusulas de confidencialidad, notificación y auditoría
Cultural	Reporte temprano de incidentes y conciencia de usuarios

La seguridad no depende de un único control. Requiere defensa en profundidad y mejora continua.

1.13 Security y toma de decisiones administrativas

Para estudiantes de administración, la seguridad debe analizarse como un proceso de decisión. No alcanza con preguntar qué herramienta se comprará. Deben formularse preguntas de gobierno.

Pregunta administrativa	Sentido de la pregunta
¿Qué activos deben protegerse con prioridad?	Permite asignar recursos según criticidad
¿Qué amenazas intencionales son más relevantes?	Permite construir escenarios de riesgo
¿Quién puede acceder a cada sistema?	Permite controlar identidades y permisos

Pregunta administrativa	Sentido de la pregunta
¿Qué proveedores tienen acceso?	Permite gestionar riesgos de terceros
¿Cómo se detecta un incidente?	Permite evaluar monitoreo real
¿Quién responde ante una alerta crítica?	Permite evitar improvisación
¿Qué evidencia se conserva?	Permite auditoría e investigación
¿Cuánto tiempo puede estar caído un sistema?	Permite definir continuidad
¿Cuánto riesgo residual se acepta?	Permite alinear seguridad con estrategia

Estas preguntas muestran que security forma parte de la administración del riesgo. La tecnología aporta herramientas, pero la organización debe decidir prioridades, responsabilidades y niveles aceptables de exposición.

1.14 Indicadores de security en TI

La seguridad debe medirse. Sin indicadores, la organización solo tiene percepciones. Algunos indicadores útiles son:

Indicador	Qué permite observar
Porcentaje de sistemas críticos con MFA	Nivel de protección de accesos
Cantidad de intentos de phishing reportados	Cultura de detección y exposición del usuario
Tiempo medio de detección de incidentes	Capacidad de monitoreo
Tiempo medio de respuesta	Capacidad de contención
Vulnerabilidades críticas abiertas	Exposición técnica
Usuarios con privilegios excesivos	Riesgo de abuso o compromiso de cuentas

Indicador	Qué permite observar
Proveedores con accesos activos	Riesgo de terceros
Backups restaurados con éxito	Capacidad de recuperación
Dispositivos sin actualización	Superficie de ataque
Alertas críticas no investigadas	Debilidad operativa del monitoreo

Estos indicadores deben ser comprensibles para la dirección. No se trata de presentar solo datos técnicos, sino de mostrar qué riesgos aumentan, qué controles funcionan y qué decisiones se requieren.

1.15 Seguridad, resiliencia y gestión organizacional

La seguridad se vincula estrechamente con la resiliencia organizacional. La resiliencia es la capacidad de anticipar, resistir, responder y recuperarse frente a eventos adversos.

En TI, una organización resiliente no es aquella que nunca sufre incidentes. Es aquella que puede reducir su probabilidad, detectarlos temprano, contenerlos, sostener funciones críticas y aprender de lo ocurrido.

Capacidad	Aplicación en security
Anticipar	Identificar amenazas, vulnerabilidades y escenarios
Resistir	Implementar controles preventivos y arquitectura segura
Detectar	Monitorear sistemas, usuarios y eventos
Responder	Activar procedimientos de contención
Recuperar	Restaurar servicios, datos y operaciones
Aprender	Revisar causas, controles y responsabilidades

La seguridad debe integrarse con continuidad del negocio, gestión de crisis, auditoría, cumplimiento normativo, capacitación y gobierno de proveedores.

1.16 Errores frecuentes al gestionar security

Algunas organizaciones cometen errores que reducen la efectividad de la seguridad.

Error	Consecuencia
Tratar security como un problema exclusivamente técnico	La dirección no asume decisiones estratégicas
Confiar solo en herramientas	Se descuidan procesos, personas y monitoreo
No inventariar activos	No se protege lo que no se conoce
No revisar accesos	Se acumulan permisos indebidos
No monitorear alertas	Los incidentes pasan desapercibidos
No capacitar usuarios	Aumenta el éxito del phishing y errores de manejo
No controlar proveedores	Se abren accesos externos no gestionados
No probar backups	La recuperación puede fallar
No documentar incidentes	Se pierde aprendizaje y evidencia
No medir	No se conoce el nivel real de exposición

La seguridad efectiva requiere una combinación de tecnología, gestión, cultura, contratos, controles y evidencia.

1.17 Criterios para una gestión adecuada de security

Una gestión adecuada de security en TI debería incluir:

- Inventario de activos críticos.
- Clasificación de información.

- Gestión de identidades y accesos.
- Autenticación multifactor.
- Segmentación de redes.
- Protección de dispositivos finales.
- Gestión de vulnerabilidades.
- Monitoreo y detección.
- Respuesta a incidentes.
- Backups probados.
- Gestión de proveedores.
- Capacitación de usuarios.
- Políticas de seguridad.
- Métricas para dirección.
- Auditoría y mejora continua.

Esta lista no implica que todas las organizaciones deban tener el mismo nivel de sofisticación. Una empresa pequeña, una universidad, una entidad financiera o una industria tendrán necesidades distintas. Lo importante es que cada organización defina controles proporcionales a sus riesgos.

2 Amenazas, vulnerabilidades y riesgo

Para comprender la seguridad de los sistemas de información conviene analizar la relación entre **amenazas**, **vulnerabilidades**, **medios de control** y **valor de la información**. El tema principal es cómo las organizaciones deben identificar los riesgos que afectan a sus sistemas y aplicar mecanismos de seguridad para proteger sus activos informacionales.

Desde la mirada de las **Tecnologías de la Información (Information Technology / Tecnologías de la Información)**, este enfoque permite comprender que la seguridad no consiste solo en instalar herramientas técnicas, sino en administrar de manera sistemática los riesgos que pueden afectar la información, los procesos, los usuarios y la continuidad operativa.

2.1 El objetivo: preservar el valor de la información

El objetivo central es **preservar el valor de la información**. En una organización, la información tiene valor porque permite tomar decisiones, operar procesos, atender clientes, cumplir obligaciones legales, gestionar recursos y sostener la actividad diaria.

Por ejemplo, una base de datos de clientes, un sistema de facturación, los registros contables, los legajos del personal o los contratos digitalizados no son simples archivos: son activos organizacionales. Si se pierden, se alteran o se divulgan indebidamente, la organización puede sufrir daños económicos, legales, operativos y reputacionales.

Por eso, la seguridad de la información busca proteger tres principios fundamentales:

Principio	Sigla en inglés	Explicación
Confidencialidad	**Confidentiality**	La información solo debe ser accesible para personas autorizadas.
Integridad	**Integrity**	La información debe mantenerse completa, exacta y no alterada indebidamente.
Disponibilidad	**Availability**	La información y los sistemas deben estar disponibles cuando se los necesita.

Estos tres principios suelen conocerse como la **tríada CIA (Confidentiality, Integrity and Availability / Confidencialidad, Integridad y Disponibilidad)**.

2.2 Amenazas: aquello que puede causar daño

Las amenazas pueden distinguirse según su **origen**. Pueden ser internas o externas. Esta distinción es muy importante para los estudiantes de administración, porque permite comprender que los riesgos no provienen únicamente de atacantes externos. Muchas veces, los problemas nacen dentro de la propia organización.

2.2.1 Amenazas internas

Las **amenazas internas** provienen de personas, procesos o recursos que forman parte de la organización. Pueden originarse en empleados, usuarios, administradores de sistemas, proveedores internos o personas con acceso legítimo a la información.

Ejemplos:

Amenaza interna	Explicación
Errores del usuario	Cargar mal una factura, borrar un archivo, enviar información confidencial al destinatario equivocado.
Abuso de privilegios	Un usuario utiliza permisos superiores a los necesarios para consultar, modificar o extraer información.
Fallas de procesos de TI	Un procedimiento mal diseñado permite omisiones, duplicaciones o accesos indebidos.

El abuso de privilegios es especialmente relevante. Un usuario puede tener acceso válido al sistema, pero utilizarlo de manera incorrecta. Por ejemplo, un empleado del área administrativa podría consultar datos salariales sin necesidad funcional o descargar información de clientes sin autorización.

2.2.2 Amenazas externas

Las **amenazas externas** provienen de actores o eventos ajenos a la organización. Ejemplos típicos son los ciberataques, el malware y los desastres naturales.

Amenaza externa	Explicación
Ciberataques (Cyberattacks / Ataques informáticos)	Intentos de ingresar, dañar, interrumpir o robar información mediante medios tecnológicos.
Hackers (Hackers / Intrusos informáticos)	Personas que intentan acceder a sistemas sin autorización.
Malware (Malicious Software / Software malicioso)	Programas diseñados para dañar, robar información o tomar control de sistemas.
Ransomware (Ransomware / Secuestro digital de información)	Tipo de malware que cifra datos y exige un pago para recuperarlos.
Desastres naturales	Inundaciones, incendios, tormentas o eventos físicos que afectan infraestructura tecnológica.

Un ejemplo administrativo claro sería una empresa que no puede facturar durante varios días porque sus servidores fueron cifrados por ransomware. El problema no es solamente técnico: afecta ventas, cobranzas, atención al cliente, cumplimiento fiscal y reputación.

2.3 Amenazas involuntarias y provocadas

También se diferencian las amenazas **involuntarias** de las **provocadas**.

Las amenazas involuntarias son aquellas que no tienen intención maliciosa. Pueden surgir por error humano, desconocimiento, cansancio, falta de capacitación o procesos mal diseñados.

Ejemplos:

- Un usuario elimina accidentalmente una carpeta compartida.
- Un empleado carga mal el CBU de un proveedor.
- Un administrador configura incorrectamente los permisos de acceso.
- Un archivo con datos personales se comparte públicamente por error.

Las amenazas provocadas, en cambio, responden a una acción deliberada. Allí aparece la figura del ciberataque, el sabotaje o la manipulación intencional de información.

Ejemplos:

- Un atacante intenta ingresar al sistema para robar credenciales.
- Un exempleado conserva accesos activos y elimina información.
- Un usuario interno copia una base de datos antes de renunciar.
- Un grupo externo ejecuta un ataque de denegación de servicio.

La diferencia es importante porque las respuestas administrativas no son iguales. Para amenazas involuntarias se requieren capacitación, validaciones, controles de proceso y supervisión. Para amenazas provocadas se necesitan controles de acceso, monitoreo, segregación de funciones, investigación y respuesta ante incidentes.

2.4 Vulnerabilidades: los puntos débiles del sistema

Las **vulnerabilidades (Weak Points / Puntos débiles)** son un elemento central. Una vulnerabilidad es una debilidad que puede ser explotada por una amenaza.

No toda amenaza produce daño por sí sola. Para que el daño ocurra, normalmente debe existir una vulnerabilidad.

Por ejemplo:

Amenaza	Vulnerabilidad	Posible consecuencia
Phishing	Usuarios sin capacitación	Robo de credenciales.
Malware	Equipos sin actualización	Infección de la red.
Abuso interno	Permisos excesivos	Acceso indebido a información sensible.
Corte eléctrico	Falta de UPS o respaldo	Interrupción del sistema.
Error de carga	Ausencia de validaciones	Información incorrecta en reportes.

Desde la mirada de administración, la vulnerabilidad no siempre es técnica. También puede ser organizacional.

Ejemplos de vulnerabilidades organizacionales:

- No existe una política formal de seguridad.
- No se revisan periódicamente los permisos de los usuarios.
- No se dan de baja los accesos de empleados desvinculados.
- No hay copias de respaldo probadas.
- Los usuarios comparten contraseñas.
- No hay separación entre quien carga, autoriza y paga.
- No existen procedimientos claros ante incidentes.

2.5 Medios de control: mecanismos para reducir el riesgo

Los **medios de control (Security Mechanisms / Mecanismos de seguridad)** son el conjunto de herramientas y procedimientos que se aplican para reducir amenazas y vulnerabilidades.

Estos controles se dividen en tres grandes grupos:

- **Controles técnicos.**
- **Controles administrativos.**
- **Controles físicos.**

Esta clasificación es muy útil para los estudiantes de administración porque muestra que la seguridad no depende únicamente del área técnica. La organización completa participa en la protección de la información.

2.6 Controles técnicos

Los **controles técnicos (Technical Controls / Controles técnicos)** son mecanismos implementados mediante hardware, software, redes, configuraciones y herramientas informáticas.

Suelen asociarse con elementos como firewalls, cifrado y servidores protegidos.

Ejemplos:

Control técnico	Función
Firewall (Firewall / Cortafuegos)	Filtra tráfico entre redes y bloquea conexiones no autorizadas.
MFA (Multi-Factor Authentication / Autenticación multifactor)	Exige más de un factor para verificar la identidad del usuario.
Cifrado (Encryption / Encriptación o cifrado)	Protege datos para que no puedan ser leídos sin una clave.
IDS (Intrusion Detection System / Sistema de detección de intrusos)	Detecta actividad sospechosa en redes o sistemas.

Control técnico	Función
IPS (Intrusion Prevention System / Sistema de prevención de intrusos)	Además de detectar, puede bloquear ataques.
Backups (Backups / Copias de respaldo)	Permiten recuperar información ante pérdida, daño o ataque.
SIEM (Security Information and Event Management / Gestión de eventos e información de seguridad)	Centraliza registros y genera alertas de seguridad.

Ejemplo: si una empresa implementa autenticación multifactor para acceder al sistema de gestión, reduce el riesgo de que una contraseña robada sea suficiente para ingresar.

2.7 Controles administrativos

Los **controles administrativos (Administrative Controls / Controles administrativos)** son políticas, normas, procedimientos y decisiones de gestión que regulan el comportamiento de las personas y el uso de los sistemas.

Se vinculan con documentos, capacitación y listas de control.

Ejemplos:

Control administrativo	Finalidad
Política de seguridad de la información	Establece reglas generales de protección.
Procedimiento de alta y baja de usuarios	Controla el ciclo de vida de los accesos.
Segregación de funciones	Evita que una persona concentre tareas incompatibles.
Capacitación en seguridad	Reduce errores y mejora la detección de incidentes.

Control administrativo	Finalidad
Auditorías periódicas	Verifican si los controles funcionan.
Política de contraseñas	Define requisitos mínimos de autenticación.
Plan de respuesta ante incidentes	Indica qué hacer cuando ocurre un problema.

Ejemplo: si un empleado deja la organización, debe existir un procedimiento para revocar inmediatamente sus accesos. Si esa baja no se realiza, se genera una vulnerabilidad administrativa.

2.8 Controles físicos

Los **controles físicos (Physical Controls / Controles físicos)** protegen instalaciones, equipos, documentos y espacios críticos.

Incluyen elementos como cámaras, lectores biométricos y cerraduras.

Ejemplos:

Control físico	Función
Cámaras de seguridad	Monitorean áreas sensibles.
Cerraduras electrónicas	Restringen el acceso físico.
Control biométrico	Verifica identidad mediante rasgos físicos.
Tarjetas de proximidad	Regulan ingreso a sectores restringidos.
Sensores de humo	Detectan riesgos ambientales.

Control físico	Función
UPS (Uninterruptible Power Supply / Sistema de alimentación ininterrumpida)	Mantiene equipos encendidos ante cortes eléctricos.
Sala de servidores protegida	Reduce riesgo de acceso indebido o daño físico.

Ejemplo: no sirve tener contraseñas seguras si cualquier persona puede ingresar físicamente a la sala donde están los servidores y manipularlos.

2.9 Relación entre amenazas, vulnerabilidades y controles

Existe una relación dinámica: las amenazas intentan afectar el valor de la información, las vulnerabilidades son puntos débiles que facilitan el daño, y los controles actúan como barreras de protección.

Desde una perspectiva de gestión, puede expresarse así:

Riesgo = Amenaza + Vulnerabilidad + Impacto potencial

Si existe una amenaza pero no hay vulnerabilidad relevante, el riesgo disminuye. Si existe una vulnerabilidad pero no hay amenaza probable, el riesgo puede ser menor. Pero cuando una amenaza concreta encuentra una vulnerabilidad importante sobre un activo crítico, el riesgo aumenta.

Ejemplo:

- Activo: sistema de facturación.
- Amenaza: ransomware.
- Vulnerabilidad: equipos sin actualización y usuarios sin capacitación.
- Impacto: imposibilidad de facturar, pérdida de ingresos y daño reputacional.

- Controles: backups, capacitación, MFA, antivirus, monitoreo y plan de contingencia.

2.10 El enfoque que debe tener la administración

Para un estudiante de licenciatura en administración, el tema no debe abordarse como una simple lista de herramientas técnicas. La pregunta administrativa es: ¿cómo se gobierna el riesgo tecnológico dentro de la organización?

Esto implica considerar:

- Qué información es crítica.
- Qué amenazas pueden afectarla.
- Qué vulnerabilidades existen.
- Qué controles ya están implementados.
- Qué controles faltan.
- Qué costo tiene proteger.
- Qué costo tendría no proteger.
- Quién es responsable.
- Cómo se mide la eficacia de los controles.
- Cómo se responde ante incidentes.
- Cómo se asegura la continuidad operativa.

La seguridad de la información debe formar parte de la gestión organizacional. No es solo un problema del área de sistemas. También involucra dirección, administración, recursos humanos, legales, auditoría, operaciones y usuarios.

2.11 Ejemplo integrador

Una empresa mediana utiliza un sistema de gestión para ventas, compras, inventario, facturación y contabilidad. El sistema contiene datos de clientes, proveedores, precios, cuentas corrientes y reportes financieros.

2.11.1 Situación de riesgo

Un empleado recibe un correo falso que simula provenir del área de soporte técnico. El mensaje solicita ingresar usuario y contraseña para "evitar el bloqueo de la cuenta". El empleado accede al enlace y carga sus credenciales.

2.11.2 Análisis

Elemento	Aplicación al caso
Activo de información	Sistema de gestión y base de datos comercial.
Amenaza	Phishing.
Vulnerabilidad humana	Usuario sin capacitación suficiente.
Vulnerabilidad técnica	Falta de autenticación multifactor.
Impacto posible	Acceso indebido, robo de datos, manipulación de operaciones.
Control técnico	MFA, filtros antiphishing, monitoreo de accesos.
Control administrativo	Capacitación, política de reporte de incidentes.
Control detectivo	Logs y alertas por ingreso inusual.
Control recuperatorio	Backup y plan de respuesta ante incidentes.

Este ejemplo muestra que la solución no es únicamente tecnológica. También se requiere formación del usuario, políticas claras, monitoreo, revisión de accesos y procedimientos de respuesta.

2.12 Importancia de la defensa en profundidad

Una idea fundamental es que los controles deben funcionar como capas. A esto se lo denomina **Defense in Depth (Defensa en profundidad)**.

La defensa en profundidad significa que la organización no depende de un único mecanismo de seguridad. Si falla una capa, otra puede reducir el impacto.

Ejemplo de capas:

- Capacitación del usuario.
- Filtro antiphishing.
- Autenticación multifactor.
- Restricción de permisos.
- Monitoreo de accesos.
- Alertas de comportamiento anómalo.
- Backup.
- Plan de respuesta ante incidentes.

Esta lógica es especialmente importante para la administración, porque permite justificar inversiones en seguridad no como gastos aislados, sino como componentes de un sistema de control.

2.13 Las vulnerabilidades en detalle

Una vulnerabilidad es una debilidad que puede ser aprovechada por una amenaza para afectar un sistema de información. Puede ser técnica, física, humana, organizacional o

procedimental. No equivale al daño mismo. Tampoco equivale a la amenaza. La amenaza es el evento o actor con capacidad de causar daño. La vulnerabilidad es la condición que permite o facilita ese daño.

Desde la administración de Tecnologías de la Información, las vulnerabilidades pueden aparecer en hardware, software, redes, bases de datos, usuarios, procesos, documentación, controles, mantenimiento, auditoría, proveedores y espacios físicos. Un sistema puede ser vulnerable por una contraseña débil, una puerta abierta, una conexión defectuosa, un programa sin actualización, un procedimiento no auditado, una mala separación de funciones o una política de seguridad mal diseñada.

Para estudiantes de administración de empresas, el concepto es central porque permite vincular tecnología, control interno y gestión del riesgo. Una organización no administra solamente amenazas externas. También administra sus propias debilidades. Si esas debilidades no se identifican, documentan y corrigen, cualquier amenaza puede producir un impacto mayor.

La vulnerabilidad permite comprender por qué la seguridad absoluta no es posible. Los sistemas son complejos, cambian de manera constante y dependen de personas, procesos y proveedores. Por eso, la gestión debe orientarse a reducir vulnerabilidades, medir el riesgo residual y revisar los controles en forma periódica.

2.13.1 Complejidad de los sistemas

La complejidad es una fuente frecuente de vulnerabilidad. Los sistemas de información actuales integran aplicaciones, bases de datos, redes, usuarios internos, proveedores, servicios en la nube, dispositivos móviles, interfaces, permisos y procesos administrativos.

Cuanto mayor es la cantidad de componentes, mayor es la posibilidad de errores de configuración, fallas de comunicación, permisos incorrectos o controles incompletos.

Fuente de complejidad	Vulnerabilidad posible	Consecuencia administrativa
Integraciones entre sistemas	Datos incompletos o duplicados	Reportes incorrectos
Múltiples perfiles de usuario	Permisos mal asignados	Accesos indebidos
Servicios en la nube	Dependencia de terceros	Riesgo de disponibilidad o confidencialidad
Procesos automatizados	Errores no detectados	Decisiones basadas en datos incorrectos
Configuraciones no documentadas	Dificultad para corregir fallas	Mayor tiempo de recuperación

Un sistema de ventas puede estar integrado con stock, facturación, cobranzas, logística y reportes gerenciales. Si un dato se carga mal en el módulo inicial, el error puede trasladarse a varios procesos. Si una integración falla, puede generarse información incompleta. Si los permisos no están bien definidos, un usuario puede modificar datos que no corresponden a su función.

La administración debe reducir la complejidad innecesaria. Esto no significa usar sistemas simples cuando la operación exige herramientas avanzadas. Significa documentar procesos, definir responsables, controlar cambios, revisar integraciones y evitar configuraciones que nadie comprende.

2.13.2 Procedimientos computarizados no auditados

Un procedimiento computarizado no auditado es una rutina, proceso, cálculo o flujo digital que se ejecuta sin revisión suficiente. Puede tratarse de una liquidación de sueldos, un cálculo de intereses, una actualización masiva de precios, una conciliación automática, una validación de descuentos o una integración entre sistemas.

La falta de auditoría permite que los errores permanezcan ocultos. Un algoritmo de cálculo mal configurado puede generar diferencias durante meses. Un proceso automático que importa pagos puede duplicar registros. Una validación incompleta puede aceptar datos erróneos.

Procedimiento	Vulnerabilidad	Control necesario
Liquidación de sueldos	Fórmula incorrecta o regla desactualizada	Revisión de casos, aprobación y conciliación
Actualización masiva de precios	Archivo incorrecto o criterio equivocado	Prueba previa, respaldo y registro de ejecución
Conciliación automática	Omisión de diferencias	Revisión de excepciones
Cálculo de intereses	Tasa mal configurada	Validación por área responsable
Integración entre sistemas	Duplicación o pérdida de datos	Controles de consistencia y reportes

Desde administración, todo procedimiento relevante debe tener controles. Puede incluir pruebas previas, revisión de resultados, trazabilidad, conciliaciones, registros de ejecución y aprobación del área responsable.

Ejemplo: si un sistema actualiza 5.000 precios, debe quedar registro de fecha, usuario, criterio aplicado, archivo utilizado y resultado final. Además, debería existir una instancia de verificación posterior.

2.13.3 Extensión de los efectos de los desastres

Una vulnerabilidad importante aparece cuando la organización no limita el alcance de un desastre. Un incendio, una inundación, una falla eléctrica, un ataque de cifrado no autorizado o una caída de comunicaciones puede afectar mucho más que el activo inicial si no existen barreras, respaldos y planes de recuperación.

La extensión del daño depende de la arquitectura y de los controles. Si los respaldos están en el mismo servidor afectado, el desastre puede destruir datos productivos y copias. Si todas las sucursales dependen de un único enlace sin alternativa, una falla central puede detener toda la operación. Si no existe plan de continuidad, cada área improvisará.

Situación vulnerable	Efecto posible	Control recomendado
Backups guardados en el mismo servidor	Pérdida simultánea de datos y copias	Copias externas o inmutables
Único enlace de comunicaciones	Interrupción total de sucursales	Conectividad alternativa
Sin plan de continuidad	Respuesta improvisada	Procedimientos documentados y probados
Sin prioridades de recuperación	Recursos asignados de forma desordenada	Clasificación de procesos críticos
Sin pruebas de restauración	Falsa sensación de seguridad	Simulacros y pruebas periódicas

La continuidad operativa requiere definir RTO y RPO. El RTO indica cuánto tiempo puede estar caído un servicio. El RPO indica cuánta información puede perderse medida en tiempo.

Si el RTO de facturación es de cuatro horas, el plan debe permitir recuperar el servicio dentro de ese plazo. Si el RPO es de una hora, los respaldos diarios no son suficientes.

2.13.4 Acceso no autorizado e identificación del usuario

El posible acceso no autorizado es una vulnerabilidad cuando los sistemas no identifican correctamente a sus usuarios o no delimitan sus permisos.

La gestión de accesos puede analizarse en tres niveles: identificación, autenticación y autorización.

Nivel	Pregunta que responde	Ejemplo
Identificación	¿Quién dice ser el usuario?	Nombre de usuario o número de legajo
Autenticación	¿Cómo se comprueba esa identidad?	Contraseña, token, código o biometría
Autorización	¿Qué puede hacer ese usuario?	Consultar, modificar, aprobar o eliminar datos

Los problemas de identificación surgen cuando se usan cuentas genéricas, usuarios compartidos o registros incompletos. Si cinco personas usan la misma cuenta, no puede saberse quién ejecutó una acción.

Los problemas de autenticación aparecen con contraseñas débiles, ausencia de autenticación multifactor, cuentas sin bloqueo por intentos fallidos o recuperación insegura de claves.

Los problemas de autorización aparecen cuando los usuarios tienen permisos superiores a los necesarios o conservan accesos de funciones anteriores.

Debilidad	Riesgo asociado	Control sugerido
Cuentas compartidas	Falta de trazabilidad	Usuarios individuales
Contraseñas débiles	Acceso indebido	Políticas de clave y MFA
Usuarios desvinculados activos	Uso indebido de cuentas	Baja inmediata
Permisos excesivos	Fraude o error	Principio de mínimo privilegio
Falta de revisión de accesos	Acumulación de privilegios	Revisiones periódicas

Un control básico consiste en revisar cada noventa días los usuarios comunes y cada treinta días las cuentas privilegiadas.

2.13.5 Vulnerabilidades físicas y conexiones defectuosas

Las vulnerabilidades físicas afectan equipos, soportes, instalaciones y condiciones ambientales. Incluyen acceso no controlado a salas, cableado expuesto, ubicación insegura de servidores, falta de protección eléctrica, soportes sin custodia y conexiones defectuosas de hardware.

También pueden existir daños por temperatura, humedad, polvo, interferencia electromagnética o exposición ambiental. En oficinas comunes, algunos riesgos pueden parecer poco frecuentes, pero deben considerarse en centros de datos, laboratorios, depósitos de respaldos, instalaciones industriales o ambientes con equipamiento crítico.

Vulnerabilidad física	Posible consecuencia	Control
Sala técnica sin control de acceso	Manipulación de equipos	Cerraduras, tarjetas y registro de ingreso
Cableado desordenado o expuesto	Cortes o fallas intermitentes	Canalización, etiquetado y mantenimiento
Servidor ubicado en zona insegura	Robo, daño o interrupción	Ubicación protegida
Falta de protección eléctrica	Daño de equipos	UPS y protectores de tensión
Soportes de respaldo sin custodia	Pérdida o fuga de información	Inventario y almacenamiento seguro

Las conexiones defectuosas pueden generar interrupciones, pérdida de paquetes, errores de lectura, fallas intermitentes y daño en equipos. Muchas veces son difíciles de detectar porque no aparecen en forma constante. Por eso resultan importantes el mantenimiento

preventivo, el orden del cableado, el inventario, las pruebas periódicas y los registros de incidentes.

2.13.6 Fallas de protección y control en software

El software puede contener debilidades de diseño, configuración o implementación. Una falla de protección puede permitir que un usuario vea datos restringidos. Una falla de control puede aceptar importes inválidos, modificar registros sin autorización o ejecutar operaciones sin registrar quién las realizó.

Los controles de aplicación son esenciales. Deben validar datos, limitar permisos, registrar operaciones, exigir aprobaciones y bloquear acciones incompatibles.

Falla en software	Riesgo	Control de aplicación
Permite aprobar operaciones sin autorización	Fraude o error	Reglas de aprobación
Acepta importes negativos incorrectos	Datos inválidos	Validación de campos
No registra modificaciones	Falta de trazabilidad	Log de auditoría
Permite exportar bases completas	Fuga de información	Restricción de exportación
No verifica presupuesto disponible	Compras sin control	Validación presupuestaria

Ejemplo: un sistema de compras permite aprobar órdenes sin verificar presupuesto disponible. El problema no es solo técnico. Es una vulnerabilidad de control administrativo dentro del software.

Otro ejemplo: una aplicación permite exportar toda la base de clientes sin registrar la descarga. Esa falla facilita robo o copia de archivos.

2.13.7 Robo y copia no autorizada de archivos

El robo y la copia no autorizada de archivos ocurren cuando una persona extrae información sin permiso o fuera de su función. Puede usar dispositivos externos, correo electrónico, almacenamiento en la nube, capturas de pantalla, impresiones o accesos remotos.

La copia no autorizada es difícil de detectar porque muchas veces el archivo original permanece intacto. Por eso, el problema no siempre se advierte de inmediato.

Tipo de archivo	Riesgo principal	Control recomendado
Base de clientes	Pérdida de confidencialidad y reclamos	Clasificación, permisos y registros
Nómina o legajos	Exposición de datos personales	Acceso restringido y cifrado
Contratos	Incumplimiento de confidencialidad	Control de versiones y permisos
Listas de precios	Daño competitivo	Restricción de exportación
Documentación contable	Uso indebido o alteración	Repositorio controlado
Claves o credenciales	Acceso a otros sistemas	Prohibición de almacenamiento inseguro

Los controles incluyen permisos mínimos, cifrado, monitoreo de descargas, bloqueo de dispositivos no autorizados, prevención de pérdida de datos, registros de acceso y acuerdos de confidencialidad. La clasificación de información permite decidir qué archivos requieren mayor protección.

2.13.8 Modificaciones al código y controles desactivados

Las modificaciones al código son vulnerabilidades cuando no están autorizadas, no fueron probadas o eliminan controles. Un cambio pequeño puede afectar seguridad, cálculos, permisos, integraciones o reportes.

Un caso crítico ocurre cuando se desmantelan módulos de protección. Puede suceder por urgencia, desconocimiento, mala práctica o intención indebida. Por ejemplo, desactivar una validación de permisos para resolver un problema temporal y dejarla inactiva en producción. También puede ocurrir que se eliminen registros de auditoría para mejorar rendimiento sin evaluar las consecuencias.

Situación	Vulnerabilidad generada	Control
Cambio sin aprobación	Riesgo de error o abuso	Gestión formal de cambios
Cambio sin prueba	Fallas en producción	Ambiente de prueba
Validación desactivada	Acceso o cálculo indebido	Revisión funcional
Log eliminado	Falta de evidencia	Auditoría técnica
Programador modifica producción directamente	Ausencia de control independiente	Separación de ambientes

El desarrollo seguro requiere separación de ambientes, revisión de código, aprobación del responsable, pruebas, control de versiones, documentación y posibilidad de reversión. Quien desarrolla no debería modificar producción sin control independiente en sistemas críticos.

2.13.9 Personal de mantenimiento y operadores

El personal de mantenimiento puede afectar el funcionamiento del sistema si realiza tareas sin procedimiento, sin registro o sin conocimiento del impacto. Una actualización de firmware, un cambio de disco, una limpieza de equipo, una modificación de configuración o una intervención sobre cableado puede generar fallas si no existe control.

Los operadores también pueden convertirse en fuente de vulnerabilidad cuando no notifican errores. Un mensaje de falla ignorado, una carga incompleta, una alerta omitida o una operación repetida sin informar puede ocultar problemas.

Actor	Vulnerabilidad posible	Control
Personal de mantenimiento	Intervención sin registro	Orden de trabajo y evidencia
Operador del sistema	Error no reportado	Procedimiento de escalamiento
Técnico externo	Acceso excesivo o no monitoreado	Autorización temporal y registro
Administrador del sistema	Cambios sin revisión	Separación de funciones
Usuario avanzado	Uso de permisos fuera de su función	Revisión periódica de perfiles

La organización debe definir procedimientos de mantenimiento, ventanas de intervención, responsables, registros y criterios de escalamiento. También debe establecer una cultura de reporte. Notificar errores no debe percibirse como una falta automática. La omisión de reporte sí debe tratarse como un riesgo serio.

2.13.10 Agujeros de seguridad e incompatibilidades

Un agujero de seguridad es una debilidad que permite acceso, daño o uso indebido. Puede ser físico, lógico o de compatibilidad.

Un agujero físico puede ser una sala sin control, un rack abierto, un puerto de red activo en un área pública o un depósito de respaldos sin custodia. Un agujero de software puede ser una vulnerabilidad conocida sin corregir, una configuración insegura o una interfaz expuesta sin protección adecuada.

Las incompatibilidades también generan vulnerabilidades. Un sistema antiguo puede no soportar mecanismos modernos de autenticación. Una aplicación nueva puede no

integrarse correctamente con controles existentes. Una actualización puede romper permisos, registros o validaciones.

Tipo de agujero	Ejemplo	Control
Físico	Rack abierto o sala sin control	Seguridad física y registro de acceso
Lógico	Servicio expuesto sin protección	Configuración segura y monitoreo
De software	Versión vulnerable sin actualizar	Parches y gestión de vulnerabilidades
De compatibilidad	Sistema antiguo sin MFA	Plan de reemplazo o control compensatorio
De configuración	Parámetros por defecto	Hardening y revisión técnica

Para reducir estos agujeros se requieren inventario, pruebas, actualización, monitoreo, control de configuración y revisión periódica. Un sistema que nadie mantiene se vuelve más vulnerable con el tiempo, aunque haya funcionado correctamente durante años.

2.13.11 Filosofía de seguridad mal elegida o mal mantenida

La filosofía de seguridad es el criterio general con el que la organización decide cómo proteger sus sistemas. Puede apoyarse en confianza amplia, control por roles, mínimo privilegio, defensa en capas, tolerancia cero a ciertos riesgos o enfoque basado en riesgos.

Una mala elección puede generar vulnerabilidades. Si se adopta una política demasiado permisiva, se acumulan accesos innecesarios. Si se adopta una política excesivamente restrictiva sin facilitar el trabajo, los usuarios buscarán atajos. Si se definen controles que luego no se mantienen, la organización tendrá una seguridad aparente.

Filosofía o criterio	Riesgo si se aplica mal	Ejemplo
Confianza amplia	Accesos excesivos	Todos pueden consultar información sensible
Control extremo	Atajos informales	Usuarios comparten claves para evitar demoras
Mínimo privilegio	Requiere revisión permanente	Si no se actualiza, queda desordenado
Defensa en capas	Puede volverse compleja	Controles múltiples sin responsables claros
Enfoque basado en riesgos	Requiere evaluación real	Riesgos aceptados sin documentación

Ejemplo: exigir contraseñas complejas pero permitir cuentas compartidas contradice la seguridad real. Exigir aprobación de accesos, pero no revisar usuarios activos durante años, también debilita el sistema.

La filosofía debe ser coherente, práctica y auditada.

2.13.12 Bugs y exploits

Un bug es un error de software. Puede ser un defecto en el código, la lógica, la configuración o el comportamiento esperado de un programa. Puede causar resultados incorrectos, fallas, bloqueos o exposición de datos. No todo bug es una vulnerabilidad de seguridad, pero algunos sí lo son.

Un exploit es un código, técnica o procedimiento que aprovecha una vulnerabilidad. Puede permitir acceso indebido, ejecución de instrucciones, extracción de datos, escalamiento de privilegios o interrupción de servicios.

Concepto	Significado	Ejemplo
Bug	Error o defecto del software	El sistema calcula mal un descuento
Vulnerabilidad	Bug o debilidad explotable	El sistema permite acceder sin autorización
Exploit	Forma de aprovechar la vulnerabilidad	Código que permite ingresar como administrador
Parche	Corrección del defecto	Actualización del proveedor
Mitigación	Medida temporal para reducir riesgo	Desactivar una función vulnerable

La diferencia es importante: el bug es el defecto; el exploit es la forma de utilizarlo para obtener un resultado.

La gestión de bugs y exploits requiere inventario de software, actualizaciones, pruebas, monitoreo, análisis de vulnerabilidades, priorización y corrección. Un error crítico en un sistema expuesto a Internet requiere tratamiento más rápido que un error menor en una herramienta interna sin datos sensibles.

2.13.13 Vulnerabilidades omitidas con frecuencia

Además de las vulnerabilidades más visibles, existen debilidades que suelen quedar fuera del análisis inicial. Estas debilidades pueden ser tan importantes como una falla técnica.

Vulnerabilidad omitida	Riesgo
Documentación desactualizada	Errores al operar o recuperar sistemas
Ausencia de inventario	Desconocimiento de activos reales

Vulnerabilidad omitida	Riesgo
Dependencia de una sola persona	Interrupción si esa persona no está disponible
Backups no probados	Imposibilidad de restaurar información
Servicios externos sin evaluación	Exposición por proveedores
Permisos heredados	Accesos innecesarios
Configuraciones por defecto	Seguridad débil
Claves guardadas en archivos visibles	Acceso indebido
Uso de dispositivos personales sin control	Fuga o pérdida de información
Falta de control de calidad de datos	Decisiones basadas en información incorrecta

También debe considerarse la vulnerabilidad de los datos incorrectos. Un sistema disponible y protegido puede producir decisiones equivocadas si los datos de entrada son erróneos. La calidad de datos es parte de la seguridad desde la mirada administrativa.

Ejemplo: si el sistema de inventario muestra 300 unidades disponibles cuando solo existen 30, la organización puede vender, prometer entregas y comprar de manera equivocada. La vulnerabilidad no está en un ataque, sino en el control insuficiente sobre la calidad de información.

2.13.14 Matriz de vulnerabilidades y controles

La siguiente matriz resume las principales vulnerabilidades y los controles administrativos y técnicos que permiten reducirlas.

Vulnerabilidad	Impacto posible	Control recomendado
Complejidad no documentada	Errores, dependencia y demoras	Documentación, responsables y revisión
Procedimientos no auditados	Cálculos incorrectos o errores ocultos	Auditoría, conciliación y trazabilidad
Backups mal ubicados o no probados	Pérdida de información	Pruebas de restauración y copias externas
Cuentas compartidas	Falta de trazabilidad	Usuarios individuales
Contraseñas débiles	Acceso indebido	MFA y política de autenticación
Permisos excesivos	Fraude o error	Mínimo privilegio y revisión periódica
Cableado o infraestructura deficiente	Interrupciones	Mantenimiento preventivo
Software sin controles de aplicación	Operaciones inválidas	Validaciones, aprobaciones y logs
Copia no autorizada de archivos	Fuga de información	DLP, cifrado y monitoreo
Cambios de código sin control	Fallas o desactivación de seguridad	Gestión de cambios
Operadores que no reportan errores	Incidentes agravados	Cultura de reporte y escalamiento
Sistemas incompatibles u obsoletos	Falta de protección moderna	Actualización o reemplazo

Vulnerabilidad	Impacto posible	Control recomendado
Filosofía de seguridad incoherente	Controles aparentes	Políticas consistentes y auditadas
Bugs explotables	Acceso indebido o interrupción	Parches y gestión de vulnerabilidades
Datos de baja calidad	Decisiones incorrectas	Validaciones y controles de calidad

2.14 Síntesis del capítulo

Las vulnerabilidades son debilidades que pueden permitir o agravar el impacto de una amenaza. Pueden originarse en la complejidad de los sistemas, procedimientos no auditados, fallas físicas, errores de software, problemas de identificación, autenticación débil, cambios de código, controles desactivados, mantenimiento deficiente, operadores que no reportan errores, agujeros de seguridad, incompatibilidades, bugs y exploits.

Desde la administración, el análisis de vulnerabilidades no debe limitarse a una revisión técnica. Debe incluir procesos, personas, controles, documentación, proveedores, continuidad, calidad de datos y cultura de reporte. Un sistema puede ser técnicamente avanzado y, al mismo tiempo, vulnerable por permisos excesivos, políticas incoherentes o falta de auditoría.

La reducción de vulnerabilidades requiere método. Primero se identifican activos y procesos críticos. Luego se detectan debilidades. Después se evalúa el riesgo, se definen controles, se asignan responsables y se verifica la eficacia. El proceso debe repetirse porque los sistemas cambian, los usuarios cambian y las amenazas también.

Para estudiantes de administración de empresas, la idea central es que las vulnerabilidades muestran dónde la organización puede fallar antes de que ocurra el daño. Gestionarlas permite prevenir pérdidas, proteger información, mejorar controles internos y sostener la continuidad operativa.

La seguridad no depende solo de reaccionar ante incidentes. Depende de encontrar y reducir debilidades antes de que sean utilizadas.

3 La seguridad desde la mirada organizacional

La seguridad de la información, observada desde la organización, no puede limitarse al área técnica. Comprende decisiones de gobierno, administración del riesgo, control interno, recursos humanos, auditoría, cumplimiento normativo, cultura organizacional y gestión de proveedores.

En Tecnologías de la Información, los sistemas procesan datos, autorizan operaciones, conservan documentos, registran movimientos, administran usuarios y sostienen actividades críticas. Por esa razón, la seguridad debe ser gestionada como una responsabilidad institucional y no como una tarea aislada del área técnica.

Una organización segura no es aquella que elimina todo riesgo. Ese objetivo no es realista. Una organización segura es aquella que identifica sus activos de información, evalúa amenazas, define políticas, capacita a su personal, separa funciones incompatibles, revisa privilegios, audita controles y corrige desvíos.

El factor humano ocupa un lugar central. Muchos incidentes relevantes involucran decisiones humanas: una contraseña compartida, un permiso otorgado sin revisión, una baja de usuario demorada, una aprobación sin control, un correo engañoso aceptado, un cambio técnico no documentado o una política ignorada.

Desde la administración de empresas, la seguridad de la información debe entenderse como parte del sistema de gestión. Protege información, pero también protege procesos de negocio, continuidad operativa, reputación, cumplimiento normativo y calidad de las decisiones.

3.1 La seguridad como función organizacional

La organización define cómo se distribuyen responsabilidades, autoridad, recursos y controles. En seguridad de la información, esta estructura es decisiva. Si no se sabe quién

aprueba accesos, quién administra sistemas, quién revisa incidentes, quién conserva evidencias y quién informa riesgos, los controles técnicos pierden eficacia.

Una empresa puede tener sistemas robustos y, aun así, ser vulnerable por fallas administrativas. Por ejemplo, si Recursos Humanos informa tarde una desvinculación, una cuenta activa puede quedar expuesta. Si un responsable de área aprueba permisos sin revisar la necesidad funcional, se incumple el principio de mínimo privilegio. Si un sistema no tiene dueño definido, nadie revisa sus usuarios, configuraciones o riesgos.

La seguridad organizacional requiere roles claros. Debe distinguirse entre dueño del proceso, dueño del dato, administrador técnico, usuario final, auditor y responsable de seguridad.

Rol organizacional	Función principal	Ejemplo de responsabilidad
Dueño del proceso	Define cómo debe operar el proceso de negocio	Aprobar el circuito de pagos o compras
Dueño del dato	Determina el valor y uso permitido de la información	Definir quién puede acceder a legajos o datos de clientes
Administrador técnico	Configura y mantiene sistemas, accesos y plataformas	Crear usuarios o asignar perfiles aprobados
Usuario final	Utiliza sistemas según funciones asignadas	Registrar operaciones o consultar información autorizada
Auditor	Verifica cumplimiento y evidencia	Revisar accesos, cambios, respaldos o incidentes

Rol organizacional	Función principal	Ejemplo de responsabilidad
Responsable de seguridad	Coordina criterios, controles y seguimiento	Proponer políticas y monitorear riesgos

El área técnica puede implementar un acceso, pero no debería decidir por sí sola si un usuario necesita aprobar pagos, modificar proveedores o consultar información sensible. Esa decisión corresponde al área responsable del proceso o del dato.

3.2 Administración del riesgo

La administración del riesgo permite identificar situaciones que pueden afectar los objetivos organizacionales. En seguridad de la información, el riesgo aparece cuando una amenaza puede aprovechar una vulnerabilidad y generar impacto sobre datos, sistemas o procesos.

Una amenaza puede ser interna o externa. Una vulnerabilidad puede ser técnica, humana o procedimental. El impacto puede ser económico, legal, operativo o reputacional.

Elemento	Significado	Ejemplo
Amenaza	Evento que puede producir daño	Acceso no autorizado, fraude interno, malware
Vulnerabilidad	Debilidad que puede ser aprovechada	Contraseña débil, permisos excesivos, falta de revisión
Impacto	Consecuencia sobre la organización	Pérdida económica, sanción, interrupción o daño reputacional
Riesgo	Posibilidad de que la amenaza explote la vulnerabilidad	Modificación indebida de cuentas bancarias de proveedores

Ejemplo: si quince personas pueden modificar cuentas bancarias de proveedores, el riesgo no es abstracto. Puede traducirse en pagos indebidos, fraude, errores contables y reclamos. La respuesta administrativa puede incluir doble aprobación, registro de cambios, revisión periódica de usuarios y alertas sobre modificaciones sensibles.

Administrar riesgos implica decidir. Algunos riesgos se reducen mediante controles. Otros se aceptan, se evitan o se transfieren.

Tratamiento del riesgo	Descripción	Ejemplo
Reducir	Aplicar controles para disminuir probabilidad o impacto	Implementar doble aprobación para pagos
Aceptar	Reconocer el riesgo como tolerable	Mantener un riesgo menor con seguimiento
Evitar	Suspender o modificar la actividad riesgosa	No habilitar accesos remotos sin controles mínimos
Transferir	Derivar parte del impacto a un tercero	Contratar seguros o exigir cláusulas a proveedores

La decisión debe considerar el valor de la información, el costo de protegerla y el costo probable de perderla.

3.3 Estrategia de seguridad

La estrategia de seguridad es el conjunto de decisiones que orienta la protección de la información según los objetivos del negocio. No todas las organizaciones necesitan los mismos controles ni el mismo nivel de inversión. Una institución que administra datos personales sensibles requiere prioridades distintas de una organización que solo publica información general.

Una estrategia de seguridad debe responder preguntas concretas.

Pregunta estratégica	Finalidad
¿Qué activos son críticos?	Identificar prioridades de protección
¿Qué riesgos son inaceptables?	Definir límites de tolerancia
¿Qué controles son obligatorios?	Establecer requisitos mínimos
¿Qué presupuesto se asignará?	Vincular seguridad con recursos disponibles
¿Qué indicadores se medirán?	Evaluar cumplimiento y evolución
¿Qué responsabilidad tendrá cada área?	Evitar zonas grises y decisiones informales

Ejemplo: si el sistema de facturación no puede detenerse más de cuatro horas, la estrategia debe incluir continuidad operativa, copias de respaldo, pruebas de restauración y soporte definido. Si el objetivo es reducir accesos indebidos, la estrategia puede incluir autenticación multifactor, revisión trimestral de permisos y bloqueo inmediato de cuentas inactivas.

La estrategia evita que la seguridad quede fragmentada. Sin una dirección común, cada área puede aplicar criterios distintos, duplicar esfuerzos o dejar riesgos sin tratamiento.

3.4 Políticas de seguridad

Las políticas de seguridad son reglas formales que establecen criterios de uso, protección y control de la información. Una política debe ser clara, aprobada, comunicada, aplicable y revisada.

No alcanza con tener documentos archivados. Una política que no se comunica ni se controla no cumple su función. Tampoco resulta útil una política demasiado general, imposible de aplicar o desconectada de los procesos reales.

Política	Contenido posible
Uso aceptable de sistemas	Reglas para utilizar equipos, redes, correo y aplicaciones
Gestión de accesos	Altas, bajas, cambios de permisos y revisiones periódicas
Contraseñas y autenticación	Requisitos de claves, MFA y bloqueo por intentos fallidos
Trabajo remoto	Condiciones para acceder desde fuera de la organización
Clasificación de información	Categorías de información pública, interna, confidencial o crítica
Copias de respaldo	Frecuencia, responsables, almacenamiento y pruebas de restauración
Respuesta ante incidentes	Pasos para informar, contener, investigar y documentar eventos
Proveedores	Requisitos de seguridad, confidencialidad, accesos y evidencias

Ejemplo: una política de accesos puede establecer que todo permiso debe tener solicitud documentada, aprobación del responsable del área, fecha de alta, perfil asignado y revisión periódica. También puede exigir que las cuentas privilegiadas se revisen cada treinta días y que las cuentas comunes se revisen cada noventa días.

3.5 Regulación y cumplimiento

La regulación impone obligaciones que afectan la seguridad de la información. Puede referirse a datos personales, documentación contable, defensa del consumidor,

confidencialidad contractual, conservación de registros, notificación de incidentes o actividad específica de un sector.

En Tecnologías de la Información, el cumplimiento no consiste solo en conocer normas. Requiere transformar obligaciones en controles operativos. Si una organización debe proteger datos personales, necesita reglas de acceso, finalidad de uso, conservación, confidencialidad y respuesta ante incidentes. Si debe conservar documentación digital durante un plazo determinado, necesita repositorios confiables, control de integridad, respaldos y procedimientos de búsqueda.

Obligación o necesidad	Control operativo asociado
Proteger datos personales	Limitar accesos, registrar consultas y capacitar usuarios
Conservar documentación digital	Definir repositorios, plazos, respaldos e integridad
Cumplir contratos de confidencialidad	Clasificar información y restringir distribución
Responder ante incidentes	Establecer procedimientos, evidencias y responsables
Auditar operaciones críticas	Mantener registros, reportes y trazabilidad

El cumplimiento debe formar parte del control interno. No basta con delegarlo en asesoría legal o en el área técnica. Las áreas de negocio deben saber qué datos tratan, con qué finalidad, quién accede y durante cuánto tiempo se conservan.

3.6 Gestión colaborativa entre áreas

La seguridad organizacional requiere coordinación entre áreas. Tecnologías de la Información administra herramientas y sistemas. Recursos Humanos informa altas, cambios y bajas. Administración define circuitos de aprobación. Auditoría revisa

evidencias. Asesoría legal interpreta obligaciones. La dirección define tolerancia al riesgo y asigna recursos.

La gestión colaborativa no elimina responsabilidades individuales. Al contrario, las hace más visibles. Cada área debe conocer su función dentro del ciclo de seguridad.

Situación	Área involucrada	Responsabilidad
Alta de empleado	Recursos Humanos	Informar ingreso y puesto
Asignación de permisos	Área usuaria	Solicitar y justificar accesos
Configuración técnica	TI	Implementar perfiles aprobados
Cambio de puesto	Recursos Humanos y área usuaria	Revisar permisos anteriores y nuevos
Contratación de proveedor	Compras, Legal, TI y área usuaria	Definir cláusulas, accesos y controles
Auditoría de accesos	Auditoría y responsables de área	Revisar evidencia y corregir desvíos

Un mecanismo útil es un comité de seguridad o mesa de control con reuniones periódicas. Allí pueden revisarse incidentes, riesgos altos, accesos privilegiados, auditorías, continuidad y acciones pendientes. En organizaciones pequeñas, puede bastar una reunión formal con acta, responsables y fechas de cumplimiento.

3.7 Concientización y capacitación

La concientización busca que el personal comprenda los riesgos y las conductas esperadas. La capacitación desarrolla habilidades concretas para actuar correctamente.

Ambas son necesarias. Una persona concientizada sabe que compartir contraseñas es riesgoso. Una persona capacitada sabe cómo usar un gestor de contraseñas, reportar un correo sospechoso o clasificar un documento.

Concepto	Finalidad	Ejemplo
Concientización	Comprender la importancia del comportamiento seguro	Reconocer que una clave compartida expone a la organización
Capacitación	Aprender a ejecutar una práctica concreta	Reportar un correo sospechoso mediante el canal definido

La formación debe ser periódica, breve, medible y vinculada con tareas reales. Puede incluir módulos de veinte minutos, simulaciones controladas, evaluaciones simples y recordatorios.

Temas básicos de capacitación:

- uso seguro de contraseñas;
- autenticación multifactor;
- correos engañosos;
- clasificación de información;
- manejo de documentos;
- reporte de incidentes;
- trabajo remoto;
- uso de dispositivos personales o corporativos.

Indicadores útiles pueden ser el porcentaje de personal capacitado por trimestre, la cantidad de evaluaciones aprobadas y el número de reportes tempranos de correos sospechosos.

3.8 Personal, selección y ciclo laboral

La seguridad comienza antes del alta de un usuario. La selección de personal debe considerar la sensibilidad del puesto, el acceso a información crítica, las verificaciones laborales pertinentes, los compromisos de confidencialidad y la claridad de responsabilidades.

No todos los cargos requieren los mismos controles. Sin embargo, los puestos con acceso privilegiado o información crítica merecen revisiones más estrictas.

Durante la relación laboral, la organización debe capacitar, asignar permisos adecuados, revisar responsabilidades y controlar cambios de función. La persona debe conocer sus obligaciones de confidencialidad, uso de sistemas, reporte de incidentes y tratamiento de datos.

La salida de una persona debe estar planificada. La revocación inmediata de privilegios ante desvinculaciones o transferencias es una medida crítica.

Etapa del ciclo laboral	Control de seguridad
Selección	Evaluar sensibilidad del puesto y obligaciones de confidencialidad
Alta	Crear usuario con permisos mínimos necesarios
Desempeño habitual	Capacitar y revisar accesos periódicamente
Cambio de puesto	Retirar permisos anteriores y asignar nuevos según función

Etapa del ciclo laboral	Control de seguridad
Desvinculación	Bloquear accesos en forma inmediata
Revisión posterior	Confirmar que no queden cuentas, tokens o accesos activos

Si un usuario deja la organización, sus accesos deben bloquearse el mismo día. En ciertos casos, el bloqueo puede realizarse antes de comunicar formalmente la salida, cuando la sensibilidad del puesto lo justifique.

3.9 Separación de funciones

La separación de funciones consiste en distribuir tareas incompatibles entre distintas personas. Su objetivo es reducir errores, fraudes y abusos. Una misma persona no debería poder iniciar, aprobar, ejecutar y revisar una operación crítica sin controles compensatorios.

En sistemas de información, este principio resulta esencial. En pagos, una persona puede cargar un proveedor, otra aprobar el alta, otra autorizar el pago y otra conciliar. En gestión de usuarios, quien solicita un acceso no debería ser quien lo aprueba y audita. En desarrollo de sistemas, quien programa un cambio no debería implementarlo en producción sin revisión.

Proceso	Riesgo si no hay separación	Control sugerido
Alta de proveedores	Creación de proveedor ficticio	Aprobación por responsable y validación documental
Cambio de cuenta bancaria	Pago indebido o fraude	Doble aprobación y registro de auditoría

Proceso	Riesgo si no hay separación	Control sugerido
Creación de usuarios	Accesos indebidos	Solicitud, aprobación y revisión posterior
Cambios en sistemas	Errores o modificaciones no autorizadas	Prueba previa, autorización y plan de reversión
Conciliaciones	Ocultamiento de irregularidades	Revisión por persona distinta a quien ejecuta pagos

La separación de funciones no siempre es posible en organizaciones pequeñas. En esos casos, pueden aplicarse controles compensatorios, como revisión posterior, reportes automáticos, autorización externa o auditorías periódicas.

3.10 Auditorías periódicas y evidencia

Las auditorías periódicas verifican si las políticas y controles funcionan. Deben revisar evidencia, no solo declaraciones. La evidencia permite demostrar que un control fue aplicado.

Una auditoría puede evaluar altas y bajas de usuarios, accesos privilegiados, copias de respaldo, cambios en sistemas, incidentes, capacitación, proveedores y cumplimiento de políticas.

Elemento auditado	Evidencia esperada
Altas de usuarios	Solicitud, aprobación, fecha de alta y perfil asignado
Bajas de usuarios	Fecha de desvinculación y fecha de bloqueo

Elemento auditado	Evidencia esperada
Accesos privilegiados	Listado de usuarios, justificación y revisión vigente
Copias de respaldo	Reportes de ejecución y pruebas de restauración
Cambios en sistemas	Solicitud, aprobación, prueba, implementación y plan de reversión
Incidentes	Registro, clasificación, acciones y cierre
Capacitación	Asistencia, evaluación o constancia de cumplimiento
Proveedores	Contratos, accesos autorizados y registros de actividad

La frecuencia depende del riesgo. Los accesos administrativos pueden revisarse cada treinta días. Los usuarios comunes pueden revisarse cada noventa días. Las copias de respaldo de sistemas críticos pueden probarse mensualmente. Los controles de aplicación pueden auditarse en ciclos semestrales o anuales, según su impacto.

3.11 Estándares y buenas prácticas

Los estándares ayudan a ordenar la gestión de seguridad. Pueden incluir criterios sobre accesos, evaluación de riesgos, continuidad, clasificación de información, seguridad física, controles técnicos, auditoría y mejora continua.

Su valor consiste en brindar estructura. No deben aplicarse de manera automática ni como una lista rígida. La organización debe adaptarlos a su tamaño, actividad, riesgos, recursos y obligaciones.

Uso de estándares	Aplicación administrativa
Ordenar controles	Definir qué temas deben cubrirse
Homogeneizar criterios	Evitar decisiones aisladas por área
Facilitar auditorías	Comparar prácticas con referencias reconocidas
Mejorar la documentación	Registrar políticas, procedimientos y evidencias
Orientar la mejora continua	Detectar brechas y priorizar acciones

Un estándar no reemplaza el juicio administrativo. Sirve como guía, pero las decisiones deben relacionarse con los riesgos reales de la organización.

3.12 Lealtad, confidencialidad y factor humano

La lealtad del personal, en seguridad de la información, debe entenderse como cumplimiento de deberes de reserva, uso adecuado de recursos y respeto de las reglas organizacionales. No puede depender solo de la confianza personal. Debe apoyarse en políticas, contratos, capacitación, controles y consecuencias ante incumplimientos.

El factor humano es primordial porque las personas usan, autorizan, diseñan, configuran, revisan y administran sistemas. También pueden cometer errores. Una estrategia madura no considera a las personas solo como fuente de riesgo, sino también como parte activa del control.

Conducta humana	Efecto sobre la seguridad
Reportar un incidente a tiempo	Permite contener daños
Revisar permisos con seriedad	Reduce accesos innecesarios
Documentar cambios técnicos	Facilita auditoría y recuperación

Conducta humana	Efecto sobre la seguridad
Compartir contraseñas	Aumenta riesgo de acceso indebido
Ignorar políticas	Debilita el sistema de control
Ocultar errores	Aumenta impacto del incidente

La organización debe facilitar conductas seguras. Si reportar un incidente genera sanción automática, las personas pueden ocultarlo. Si las políticas son imposibles de cumplir, se buscarán atajos. Si los sistemas son excesivamente complejos, aumentarán los errores.

La seguridad organizacional requiere normas exigentes, pero practicables.

3.13 Modificación de formas de acceso

Las formas de acceso deben actualizarse cuando cambia el riesgo. No resulta suficiente mantener usuarios y contraseñas simples si existen accesos remotos, sistemas críticos o información sensible.

La organización puede incorporar autenticación multifactor, perfiles por rol, bloqueo por intentos fallidos, acceso condicional, registros de actividad y revisión de cuentas inactivas.

Medida de acceso	Riesgo que reduce
Autenticación multifactor	Robo o uso indebido de contraseñas
Perfiles por rol	Permisos excesivos
Bloqueo por intentos fallidos	Ataques de prueba de contraseñas
Revisión de cuentas inactivas	Accesos olvidados o innecesarios
Registros de actividad	Falta de trazabilidad
Acceso condicional	Ingresos desde ubicaciones, horarios o dispositivos no autorizados

Un caso típico es el trabajo remoto. Si el personal accede desde redes externas, deben revisarse autenticación, dispositivos autorizados, cifrado, redes privadas virtuales, registros y restricciones por ubicación u horario cuando corresponda.

Modificar accesos también implica eliminar prácticas inseguras. Las cuentas genéricas deben evitarse o justificarse. Las contraseñas compartidas deben prohibirse. Los privilegios permanentes deben reducirse. Las cuentas de emergencia deben tener control especial, registro de uso y revisión posterior.

3.14 Ejemplo integrador: cambio de cuenta bancaria de proveedor

El cambio de una cuenta bancaria de proveedor permite observar cómo se relacionan los conceptos del tema.

Elemento	Aplicación al caso
Activo protegido	Datos maestros de proveedores
Riesgo	Pago indebido o fraude
Amenaza	Modificación maliciosa o error administrativo
Vulnerabilidad	Permisos excesivos o falta de aprobación
Control preventivo	Doble aprobación y documentación respaldatoria
Control detectivo	Reporte periódico de cambios realizados
Control correctivo	Reversión, reclamo, investigación y ajuste de permisos
Evidencia	Solicitud, aprobación, usuario, fecha, motivo y documentación

Elemento	Aplicación al caso
Área involucrada	Administración, Tesorería, Compras, TI y Auditoría

Este caso muestra que la seguridad no es solo técnica. También depende del circuito administrativo, de la asignación de responsabilidades, del control interno, de la trazabilidad y de la revisión posterior.

3.15 Síntesis del capítulo

La seguridad desde la mirada organizacional demuestra que proteger información no es solo una tarea técnica. Es una función de gobierno, administración y control. Involucra dirección, Recursos Humanos, áreas usuarias, Tecnologías de la Información, auditoría, asesoría legal, proveedores y usuarios finales.

La administración del riesgo permite ordenar prioridades. La estrategia de seguridad define criterios. Las políticas establecen reglas. La regulación impone obligaciones. La capacitación mejora conductas. La separación de funciones reduce abusos. Las auditorías verifican cumplimiento. Los estándares aportan estructura. La revocación inmediata de privilegios limita accesos indebidos. La modificación de formas de acceso permite adaptar controles a nuevos escenarios.

Para estudiantes de administración de empresas, el aprendizaje central consiste en comprender que la seguridad se integra con procesos, personas y decisiones. Una organización no protege sus sistemas solo con tecnología. Los protege cuando define responsabilidades, controla accesos, capacita, documenta, audita y corrige.

El factor humano es primordial. Las personas pueden originar incidentes, pero también pueden prevenirlos, detectarlos y contenerlos. La diferencia depende del diseño organizacional. Una cultura de seguridad efectiva no se basa en declaraciones generales, sino en prácticas verificables: accesos revisados, bajas oportunas, políticas aplicadas, controles proporcionales y evidencia disponible.

4 Gestión de activos de información

Toda organización necesita recursos para funcionar. Algunos son visibles: computadoras, servidores, teléfonos, impresoras, redes, discos externos, dispositivos de almacenamiento, salas técnicas y equipos de comunicación. Otros son menos visibles, pero pueden ser todavía más importantes: bases de datos, contratos digitales, registros de clientes, legajos de personal, configuraciones de sistemas, credenciales, certificados digitales, claves de cifrado, reportes contables y documentación legal.

Todos esos elementos pueden ser considerados **activos de información** cuando permiten crear, procesar, almacenar, transmitir, proteger o utilizar información relevante para la organización. Desde la administración de Tecnologías de Información, no alcanza con saber que "hay sistemas" o que "hay datos". Se necesita conocer qué activos existen, dónde están, quién es responsable, qué valor tienen, qué riesgo generan, qué controles requieren y qué debe hacerse con ellos durante todo su ciclo de vida.

La gestión integral de activos de información puede entenderse como el conjunto de procesos mediante los cuales una organización identifica, clasifica, registra, asigna responsables, protege, audita y finalmente dispone sus activos de información. Su finalidad no es solamente ordenar inventarios. Su finalidad principal es permitir que la organización pueda proteger aquello que necesita para operar, cumplir obligaciones, tomar decisiones y sostener la continuidad del negocio.

Desde una mirada administrativa, un activo sin registro es un punto ciego. Un dato sin clasificación recibe controles inadecuados. Un sistema sin propietario funcional queda sin responsable real. Una laptop sin cifrado puede convertirse en una brecha de datos. Un proveedor que conserva información más tiempo del necesario puede generar un riesgo legal. Un soporte retirado de uso sin destrucción segura puede exponer datos años después.

Por eso, la gestión de activos de información no debe verse como una actividad puramente técnica. Es un componente del gobierno de la organización, del control interno, de la auditoría, de la seguridad de la información y de la gestión del riesgo.

4.1 Punto de partida: qué es un activo de información

Un activo de información es cualquier recurso que tiene valor para la organización porque permite operar, decidir, cumplir obligaciones, prestar servicios, controlar procesos o conservar evidencia. Puede ser tangible o intangible. Puede estar dentro de la organización o en manos de un proveedor. Puede ser un equipo físico, un archivo digital, una credencial, una aplicación o una base de datos.

La idea central es simple: **si un elemento contiene, procesa, transmite o protege información relevante, debe ser gestionado como activo**.

Tipo general de activo	Ejemplos	Riesgo principal si no se gestiona
Equipos físicos	Servidores, notebooks, celulares, discos externos	Pérdida, robo, daño físico o exposición de datos
Datos	Bases de clientes, nómina, contratos, reportes contables	Filtración, alteración, eliminación o uso indebido
Software	ERP, CRM, sistema de facturación, aplicaciones en la nube	Fallas, licencias irregulares, vulnerabilidades o dependencia operativa
Configuraciones	Reglas de firewall, parámetros de seguridad, permisos	Accesos indebidos, exposición de servicios o interrupciones
Identidades	Usuarios, cuentas administrativas, credenciales de proveedores	Abuso de permisos, fraude o acceso no autorizado

Tipo general de activo	Ejemplos	Riesgo principal si no se gestiona
Soportes	Pendrives, cintas, discos, medios ópticos	Pérdida de información, malware o incumplimiento de destrucción segura

La administración debe comprender que la seguridad comienza con el conocimiento. No se puede proteger, auditar ni recuperar aquello que no está identificado. Por eso, la gestión de activos es una condición previa para cualquier política de seguridad de la información.

4.2 Por qué la gestión de activos importa para la administración

La gestión de activos de información tiene consecuencias directas sobre la administración de empresas. No se limita a "saber cuántas computadoras hay". Permite tomar decisiones sobre inversión, riesgo, cumplimiento, continuidad, costos y responsabilidades.

Una organización que no conoce sus activos enfrenta problemas concretos:

Problema	Consecuencia administrativa
Inventario incompleto	No se sabe qué sistemas deben respaldarse, actualizarse o auditarse
Activos sin propietario	Nadie define permisos, clasificación, retención o eliminación
Información sin clasificación	Datos sensibles pueden tratarse como información común
Software no registrado	Riesgo de licencias vencidas, uso indebido o costos innecesarios
Activos en la nube no controlados	Datos críticos pueden quedar fuera de políticas corporativas

Problema	Consecuencia administrativa
Soportes sin trazabilidad	No se puede demostrar que la información fue protegida o destruida
Retención indefinida	Se acumulan datos que ya no tienen utilidad y aumentan el riesgo legal
Baja deficiente de activos	Equipos o cuentas pueden seguir activos después de terminar su uso

Para la administración, el inventario de activos es comparable al inventario de bienes físicos o al registro contable de recursos. La diferencia es que muchos activos de información son intangibles y dinámicos. Pueden crearse, modificarse o eliminarse en minutos. Por esa razón, requieren procedimientos y controles específicos.

4.3 Inventario de activos de información

El inventario de activos es el registro formal, actualizado y verificable de los recursos que la organización utiliza para operar con información. Es el punto de partida de la gestión de seguridad, auditoría, continuidad y cumplimiento.

Un inventario adecuado no debe ser una planilla aislada que se completa una vez y luego queda desactualizada. Debe ser un proceso vivo. Cada alta, baja o modificación de un activo debe reflejarse en el registro correspondiente.

4.3.1 Información mínima del inventario

Campo	Finalidad
Identificador único	Evitar confusiones entre activos similares
Nombre del activo	Permitir reconocimiento operativo
Tipo de activo	Clasificarlo como físico, lógico, software, red, nube, dato, etc.

Campo	Finalidad
Dueño funcional	Identificar quién responde por el activo desde el negocio
Custodio técnico	Identificar quién lo administra técnicamente
Ubicación física o lógica	Saber dónde está o en qué entorno opera
Nivel de criticidad	Determinar impacto si el activo falla, se pierde o se expone
Clasificación de la información	Definir si contiene datos públicos, internos, confidenciales o restringidos
Fecha de incorporación	Registrar cuándo comenzó a formar parte del ambiente
Estado actual	Activo, en mantenimiento, retirado, dado de baja o en destrucción
Controles aplicados	Cifrado, backup, monitoreo, antivirus, restricciones de acceso
Fecha de última revisión	Asegurar actualización periódica

4.3.2 Ejemplo de registro de inventario

ID	Activo	Tipo	Dueño funcional	Custodio	Criticidad	Clasificación	Estado
ACT-001	Base de clientes	Información	Gerencia	TI	Alta	Confidencial	Activo

ID	Activo	Tipo	Dueño funcional	Custodio	Criticidad	Clasificación	Estado
ACT-002	Servidor de facturación	Físico / lógico	Administración	Infraestructura	Crítica	Confidencial	Activo
ACT-003	Plataforma CRM en la nube	Software / nube	Comercial	TI / proveedor	Alta	Confidencial	Activo
ACT-004	Pendrive de respaldo mensual	Soporte removible	Finanzas	TI	Media	Restringida	En custodia
ACT-005	Notebook de gerencia	Equipo final	Dirección	Mesa de ayuda	Alta	Confidencial	Activo

Un inventario completo permite responder preguntas esenciales: qué existe, dónde está, quién lo usa, quién lo administra, qué datos contiene, qué controles tiene y qué impacto tendría su pérdida.

4.4 Tipos de activos de información

Los activos no son todos iguales. La clasificación por tipo permite aplicar controles adecuados según la naturaleza del activo y el riesgo que representa.

4.4.1 Activos físicos

Los activos físicos son los componentes materiales que soportan la infraestructura tecnológica. Incluyen servidores, computadoras de escritorio, notebooks, celulares corporativos, impresoras, dispositivos de red, discos externos, cintas, medios removibles, sistemas de energía y equipamiento de salas técnicas.

Activo físico	Riesgo frecuente	Control recomendado
Notebook	Robo o pérdida con datos internos	Cifrado de disco, bloqueo de pantalla y borrado remoto
Servidor	Daño físico o acceso no autorizado	Sala técnica cerrada, monitoreo y mantenimiento
Pendrive	Copia o traslado no autorizado de datos	Cifrado, inventario y restricción de uso
Switch o router	Manipulación de red o interrupción	Acceso físico restringido y configuración segura
UPS	Falla de energía sin respaldo	Pruebas periódicas y mantenimiento preventivo

El riesgo físico también es riesgo de información. Una computadora robada no representa solamente una pérdida económica por el valor del equipo. Puede representar una exposición de datos, credenciales, correos, documentos internos y accesos a sistemas.

4.4.2 Activos lógicos

Los activos lógicos son elementos digitales que permiten operar sistemas o proteger información. Incluyen sistemas operativos, configuraciones, scripts, certificados digitales, claves criptográficas, credenciales, bases de configuración y parámetros de seguridad.

Estos activos suelen ser menos visibles que los físicos, pero pueden ser más críticos. Un certificado digital vencido puede dejar inaccesible un portal. Una clave de cifrado perdida puede volver irrecuperables datos protegidos. Una configuración incorrecta puede exponer un sistema completo.

Activo lógico	Riesgo	Ejemplo
Certificado digital	Vencimiento o uso indebido	El sitio de clientes deja de funcionar por certificado vencido
Clave criptográfica	Pérdida o exposición	Los datos cifrados no pueden recuperarse o son accedidos por terceros
Script de automatización	Ejecución indebida	Una rutina elimina archivos por error
Configuración de firewall	Regla insegura	Se permite acceso externo a un sistema interno
Credencial administrativa	Robo o abuso	Un atacante accede con privilegios elevados

4.4.3 Activos de información

Los activos de información son los datos que la organización produce, recibe, almacena o transmite. Incluyen bases de datos, expedientes, contratos, correos, legajos, reportes, documentación legal, información contable, registros de clientes y datos de proveedores.

Su valor no siempre se mide de manera directa en dinero, pero su pérdida puede producir consecuencias financieras, legales, reputacionales y operativas.

Activo de información	Posible impacto si se compromete
Base de clientes	Reclamos, pérdida de confianza, incumplimiento de protección de datos
Nómina	Exposición de datos personales y salariales
Contratos	Conflictos legales o pérdida de evidencia
Reportes financieros	Decisiones erróneas o incumplimientos contables
Datos bancarios de proveedores	Fraude por modificación o transferencia indebida
Expedientes internos	Riesgo legal y reputacional

4.4.4 Activos de software

Los activos de software son aplicaciones, plataformas, licencias y desarrollos que la organización usa para operar. Incluyen sistemas ERP, CRM, nómina, facturación, comercio electrónico, herramientas de colaboración, software de seguridad y aplicaciones en la nube.

La administración de software incluye tanto la dimensión operativa como la legal. Usar software sin licencia válida puede generar sanciones. Mantener licencias sin uso genera costos innecesarios. Utilizar versiones obsoletas puede introducir vulnerabilidades.

Riesgo de software	Consecuencia
Licencias vencidas	Incumplimiento contractual o legal
Licencias no utilizadas	Gasto sin beneficio

Riesgo de software	Consecuencia
Software no autorizado	Malware, incompatibilidad o fuga de datos
Software sin actualización	Exposición a vulnerabilidades conocidas
Aplicaciones críticas sin soporte	Riesgo de continuidad y mantenimiento

4.4.5 Activos de red

Los activos de red permiten que usuarios, sistemas, sedes y proveedores se comuniquen. Incluyen redes locales, redes inalámbricas, conexiones a Internet, firewalls, routers, switches, VPN, IDS, IPS, proxies, balanceadores y puntos de acceso.

La gestión de activos de red requiere registrar equipos, reglas, conexiones, responsables y configuraciones. Una red no inventariada puede tener puntos de acceso no autorizados, reglas inseguras o conexiones activas que nadie supervisa.

Activo de red	Control esperado
Firewall	Reglas documentadas, aprobadas y revisadas
Router	Acceso administrativo restringido
Punto de acceso Wi-Fi	Configuración segura y autorización de TI
VPN	Usuarios autorizados, MFA y revisión de accesos
Switch	Gestión centralizada y puertos controlados
Proxy	Registro de tráfico y políticas de navegación

4.4.6 Activos en la nube

Los activos en la nube son recursos contratados o creados en plataformas externas. Pueden incluir servidores virtuales, bases de datos gestionadas, almacenamiento,

aplicaciones SaaS, entornos de desarrollo, repositorios de código, servicios de integración y herramientas de colaboración.

Su principal desafío es la visibilidad. En la nube, un área puede contratar una herramienta o crear un recurso sin pasar por TI. Esto se conoce como **TI en la sombra**. El problema no es solo que el área use una herramienta externa, sino que esa herramienta puede procesar datos críticos sin evaluación de seguridad, sin contrato adecuado, sin respaldo y sin controles de acceso.

Riesgo en nube	Ejemplo
Recurso no inventariado	Base de datos creada para un proyecto y olvidada
Configuración pública	Carpeta o repositorio accesible desde internet
SaaS contratado por un área	Herramienta de marketing con datos de clientes sin revisión de TI
Falta de control de usuarios	Ex empleados conservan acceso a una plataforma externa
Dependencia del proveedor	Dificultad para recuperar datos o migrar servicios

4.4.7 Activos humanos

Las personas también forman parte de la gestión de activos, porque acceden a sistemas, datos y procesos. Empleados, contratistas, consultores, proveedores y personal temporal representan identidades digitales que deben administrarse.

La gestión de activos humanos se relaciona con altas, bajas, modificaciones de puesto, permisos, capacitación, responsabilidades y revisión periódica de accesos.

Situación	Riesgo	Control
Alta de empleado	Permisos excesivos desde el inicio	Perfil por rol y aprobación funcional
Cambio de puesto	Acumulación de permisos anteriores	Revisión de accesos por transferencia interna
Contratista externo	Acceso mayor al necesario	Permisos temporales y monitoreados
Desvinculación	Cuenta activa después de la baja	Offboarding inmediato
Falta de capacitación	Uso inseguro de información	Formación periódica

4.5 Clasificación de la información

La clasificación de la información consiste en asignar niveles de sensibilidad a los datos para definir qué controles deben aplicarse. Sin clasificación, toda la información tiende a tratarse igual. Eso produce dos errores: proteger en exceso información de bajo riesgo y proteger en forma insuficiente información crítica.

Una clasificación simple y útil puede incluir cuatro niveles.

Nivel	Descripción	Ejemplos	Controles esperados
Pública	Puede compartirse sin restricciones	Folletos, publicaciones web, datos institucionales generales	Revisión previa de publicación

Nivel	Descripción	Ejemplos	Controles esperados
Interna	Uso dentro de la organización	Procedimientos internos, comunicaciones generales	Acceso limitado a personal autorizado
Confidencial	Su divulgación puede afectar a personas u organización	Nómina, contratos, datos de clientes, información financiera	Control de acceso, cifrado, monitoreo, restricción de reenvío
Restringida	Máxima sensibilidad y acceso muy limitado	Claves, credenciales, estrategias críticas, información judicial o de adquisición	Acceso por necesidad estricta, MFA, trazabilidad y aprobación específica

La clasificación debe estar definida por política. También debe ser comprensible para los usuarios. Si la nomenclatura es demasiado compleja, no será utilizada correctamente.

4.6 Etiquetado de la información

El etiquetado es el mecanismo que hace visible la clasificación. Consiste en marcar documentos, correos, archivos o registros con una categoría de sensibilidad.

Puede ser manual o automático:

Tipo de etiquetado	Descripción	Ventaja	Riesgo
Manual	El usuario elige la etiqueta	Permite criterio contextual	Puede depender del conocimiento o

Tipo de etiquetado	Descripción	Ventaja	Riesgo
			descuido del usuario
Automático	El sistema aplica la etiqueta según reglas	Reduce omisiones	Puede generar falsos positivos o falsos negativos
Mixto	El sistema sugiere y el usuario confirma	Equilibra automatización y criterio	Requiere capacitación y revisión

Ejemplo: un sistema puede identificar números de documento, datos bancarios o términos salariales y sugerir la etiqueta “Confidencial”. Si el usuario intenta enviar ese archivo por correo externo, la política puede bloquearlo o pedir aprobación adicional.

El etiquetado permite aplicar controles automáticos: impedir reenvíos, exigir cifrado, registrar accesos, bloquear descargas o impedir impresión.

4.7 Roles sobre los activos: propietario, custodio y usuario

La gestión de activos requiere claridad en las responsabilidades. Tres roles son fundamentales: propietario, custodio y usuario.

Rol	Función principal	Ejemplo
Propietario del activo	Define valor, clasificación, reglas de acceso, retención y uso permitido	Gerencia de Finanzas sobre la base de cuentas por pagar
Custodio del activo	Administra técnicamente el activo y ejecuta controles	Área de TI que mantiene servidores, permisos y backups

Rol	Función principal	Ejemplo
Usuario del activo	Usa el activo según su función y las reglas definidas	Analista autorizado para consultar proveedores

El propietario no siempre administra técnicamente el activo. El custodio no siempre decide las reglas de negocio. El usuario no puede otorgar accesos ni modificar la clasificación por decisión propia.

4.7.1 Ejemplo aplicado

Si se trata de una base de datos de proveedores:

Decisión o tarea	Responsable principal
Definir quién puede modificar datos bancarios	Propietario funcional
Configurar perfiles de acceso en el sistema	Custodio técnico
Usar la información para procesar pagos	Usuario autorizado
Revisar accesos periódicamente	Propietario con soporte de TI
Aplicar backup y monitoreo	Custodio técnico
Aprobar eliminación o archivo	Propietario funcional

Esta distinción evita un problema frecuente: creer que todo lo relacionado con sistemas corresponde a TI. TI administra controles técnicos, pero las reglas de negocio deben ser definidas por las áreas responsables.

4.8 Ciclo de vida de la información

La información tiene un ciclo de vida. Nace, se usa, se almacena, se transfiere, se archiva y finalmente se destruye. Cada etapa requiere controles diferentes.

Etapa	Qué ocurre	Control principal
Creación	Se genera un documento, registro, transacción o dato	Clasificación inicial y responsable asignado
Uso	La información se consulta, modifica o procesa	Control de acceso y trazabilidad
Almacenamiento	La información se guarda en repositorios	Cifrado, permisos, backup e integridad
Transferencia	La información se envía entre personas, sistemas o proveedores	Cifrado en tránsito, autenticación e integridad
Archivo	La información deja de usarse activamente pero debe conservarse	Retención, acceso restringido y conservación
Destrucción	La información llega al final de su vida útil	Borrado seguro o destrucción certificada

La etapa de destrucción suele ser subestimada. Sin embargo, es una de las más críticas. La información que ya no tiene valor operativo puede seguir teniendo valor para un atacante o generar responsabilidades legales si se conserva indebidamente.

4.9 Retención documental

La retención documental define cuánto tiempo debe conservarse cada tipo de información. Sus plazos dependen de obligaciones legales, fiscales, laborales, contractuales, regulatorias y operativas.

Conservar menos tiempo del necesario puede impedir demostrar derechos, cumplir auditorías o defender reclamos. Conservar más tiempo del necesario también genera

riesgos: aumenta el volumen de información expuesta, eleva costos de almacenamiento y puede contradecir principios de protección de datos personales.

Tipo de información	Criterio de retención
Registros contables	Plazos legales y fiscales aplicables
Legajos de personal	Normativa laboral y necesidades probatorias
Contratos	Vigencia contractual, prescripción y obligaciones legales
Correos corporativos	Política interna, litigios, auditoría y privacidad
Datos de clientes	Finalidad del tratamiento y normativa de protección de datos
Reportes operativos	Valor administrativo, histórico o probatorio

Una política de retención debe indicar:

Elemento	Contenido
Tipo documental	Qué información alcanza
Plazo mínimo	Tiempo durante el cual debe conservarse
Plazo máximo	Momento en que debe revisarse o eliminarse
Repositorio autorizado	Dónde debe conservarse
Responsable	Quién controla la retención
Procedimiento final	Archivo, revisión, anonimización o destrucción

La retención no debe quedar librada al criterio individual de cada usuario. Debe formar parte de una política institucional.

4.10 Destrucción segura y borrado seguro

Cuando la información ya no debe conservarse, corresponde eliminarla de manera segura. El simple borrado de un archivo no alcanza, porque muchas veces los datos permanecen recuperables.

4.10.1 Diferencia entre destrucción segura y borrado seguro

Concepto	Aplica a	Ejemplo	Objetivo
Destrucción segura	Soportes físicos	Triturar discos, destruir cintas, destruir papel sensible	Impedir recuperación física del soporte
Borrado seguro	Datos digitales	Sobrescritura, eliminación criptográfica, borrado certificado	Impedir recuperación lógica del dato

4.10.2 Métodos frecuentes

Método	Uso típico	Observación
Trituración física	Papel, discos, tarjetas, soportes	Debe generar certificado si interviene proveedor
Desmagnetización	Medios magnéticos	Requiere equipamiento específico
Sobrescritura	Discos y archivos	Puede no ser suficiente en ciertos dispositivos modernos

Método	Uso típico	Observación
Destrucción criptográfica	Datos cifrados	Elimina la clave que permite leer el dato
Borrado certificado por proveedor	Servicios en la nube o reciclado tecnológico	Debe estar previsto contractual y documentalmente

La destrucción segura debe dejar evidencia: fecha, activo, método, responsable, proveedor interviniente y certificado cuando corresponda. Sin evidencia, la organización no puede demostrar que la información fue efectivamente eliminada.

4.11 Soportes removibles

Los soportes removibles son dispositivos que pueden conectarse, transportarse y desconectarse con facilidad: pendrives, discos externos, tarjetas de memoria, CDs, DVDs y cintas. Su portabilidad los vuelve útiles, pero también riesgosos.

4.11.1 Riesgos principales

Riesgo	Ejemplo	Consecuencia
Extracción no autorizada	Copiar una base en un pendrive personal	Fuga de información
Introducción de malware	Conectar un dispositivo infectado	Compromiso de equipos internos
Pérdida o extravío	Olvidar un disco externo con datos de clientes	Brecha de confidencialidad
Falta de inventario	No saber quién tiene cada soporte	Ausencia de trazabilidad

Riesgo	Ejemplo	Consecuencia
Reutilización sin borrado	Entregar un disco con datos previos	Exposición accidental

4.11.2 Controles recomendados

Control	Finalidad
Bloqueo o restricción de puertos USB	Evitar uso no autorizado
Inventario de soportes corporativos	Conocer ubicación y responsable
Cifrado obligatorio	Proteger datos ante pérdida
Prohibición de dispositivos personales	Reducir malware y fuga de datos
Registro de uso	Asegurar trazabilidad
Borrado seguro antes de reutilizar	Evitar exposición de información previa
Destrucción certificada al retirar	Cerrar el ciclo de vida del soporte

Los soportes removibles deben ser tratados como activos de información, no como accesorios menores.

4.12 Gestión de activos en la nube y TI en la sombra

La nube facilita crear recursos rápidamente. Esa agilidad puede ser positiva para el negocio, pero también puede generar activos fuera del control institucional. Una base de datos creada para una prueba, una carpeta compartida con un proveedor o una aplicación contratada por un área funcional pueden contener información crítica sin estar en el inventario.

La TI en la sombra aparece cuando las áreas usan soluciones tecnológicas sin conocimiento o aprobación del área responsable de TI. No siempre surge con mala intención. Muchas veces responde a necesidades reales de velocidad o productividad. El problema es que se rompe la visibilidad del riesgo.

Situación	Riesgo
Herramienta SaaS contratada sin revisión	Datos fuera de controles corporativos
Repositorio en la nube compartido públicamente	Exposición de documentos
Usuarios dados de alta manualmente	Accesos activos después de desvinculaciones
Falta de contrato formal	Sin cláusulas de seguridad, confidencialidad o salida
Sin respaldo propio	Dependencia total del proveedor

La administración debe definir reglas claras: qué servicios pueden contratarse, quién autoriza, cómo se registran, qué datos pueden almacenarse, qué controles mínimos debe tener el proveedor y cómo se realiza la baja del servicio.

4.13 Auditoría de la gestión de activos

La auditoría verifica si la gestión de activos es real, documentada y efectiva. No alcanza con declarar que existe un inventario. Debe comprobarse si está actualizado, si los activos tienen propietario, si están clasificados, si los controles se aplican y si existe evidencia.

4.13.1 Aspectos a auditar

Aspecto	Pregunta de auditoría
Inventario	¿Todos los activos relevantes están registrados?
Propiedad	¿Cada activo tiene dueño funcional y custodio técnico?
Clasificación	¿La información está clasificada según sensibilidad?

Aspecto	Pregunta de auditoría
Etiquetado	¿La clasificación es visible y operativa?
Altas y bajas	¿Existe procedimiento para incorporar y retirar activos?
Retención	¿Los plazos documentales están definidos y aplicados?
Destrucción	¿Existen certificados o evidencias de eliminación segura?
Soportes removibles	¿Están inventariados, cifrados y controlados?
Nube	¿Los activos cloud están registrados y gobernados?
Accesos	¿Los usuarios tienen permisos adecuados al rol?

4.13.2 Hallazgos frecuentes

Hallazgo	Riesgo asociado
Servidores no registrados	Sin backup, monitoreo o actualización
Laptops retiradas sin borrado seguro	Exposición de datos
Activos sin propietario	Ausencia de decisiones sobre acceso y retención
Información confidencial sin etiqueta	Reenvío o almacenamiento inadecuado
Aplicaciones SaaS no autorizadas	Datos fuera de contratos y controles

Hallazgo	Riesgo asociado
Pendrives sin cifrado	Fuga de información ante pérdida
Licencias sin uso	Gasto innecesario
Software sin licencia	Riesgo legal
Reglas de firewall sin justificación	Exposición de red

La auditoría debe producir recomendaciones con responsables y plazos. El objetivo no es señalar fallas de manera aislada, sino mejorar la capacidad de control de la organización.

4.14 Caso integrador: notebook perdida con información confidencial

Una gerente comercial pierde una notebook durante un viaje. El equipo contenía presentaciones, contratos en negociación y una copia local de clientes estratégicos.

Elemento	Análisis
Activo físico afectado	Notebook corporativa
Activo de información afectado	Contratos, base de clientes y documentos comerciales
Riesgo	Exposición de información confidencial
Pregunta clave	¿El disco estaba cifrado?
Control preventivo	Cifrado de disco, bloqueo de pantalla, prohibición de copias locales innecesarias
Control detectivo	Registro de último acceso y alerta de conexión posterior
Control correctivo	Revocación de credenciales y bloqueo remoto

Elemento	Análisis
Control administrativo	Reporte formal del incidente y evaluación de datos contenidos
Evidencia requerida	Inventario del equipo, usuario asignado, controles activos y reporte de pérdida

El caso muestra que la gestión de activos permite responder con precisión. Si la notebook estaba inventariada, cifrada y asociada a un usuario, la organización puede actuar rápido. Si no existía registro, no se sabe qué información estaba expuesta ni qué controles estaban activos.

4.15 Caso integrador: sistema en la nube no registrado

Un área de marketing contrata una herramienta SaaS para gestionar campañas. Para funcionar, la herramienta importa datos de clientes desde el CRM. El área no informa a TI ni a legales. Meses después, se descubre que la herramienta almacena datos en servidores externos y permite el acceso de varios usuarios que ya no trabajan en la organización.

Elemento	Análisis
Activo en la nube	Plataforma SaaS contratada por marketing
Activo de información	Datos de clientes
Riesgo	Pérdida de control sobre datos personales y comerciales
Vulnerabilidad	Contratación sin evaluación de seguridad ni registro de activo
Impacto	Incumplimiento contractual, fuga de datos y accesos indebidos

Elemento	Análisis
Control preventivo	Política de aprobación de aplicaciones SaaS
Control detectivo	Monitoreo de uso de servicios no autorizados
Control correctivo	Revisión contractual, baja de usuarios y evaluación de exposición
Responsable funcional	Área propietaria del proceso comercial
Custodio técnico	TI, una vez incorporado formalmente al inventario

Este caso muestra que la tecnología puede entrar a la organización por áreas no técnicas. La administración debe equilibrar agilidad y control.

4.16 Modelo simple para aplicar en una organización

Una organización puede iniciar la gestión de activos con un modelo práctico de seis pasos.

Paso	Acción	Resultado esperado
1	Identificar activos	Lista inicial de sistemas, datos, equipos, usuarios y proveedores
2	Clasificar información	Niveles de sensibilidad asignados
3	Asignar responsables	Propietario funcional y custodio técnico definidos
4	Aplicar controles	Cifrado, backup, permisos, monitoreo y retención

Paso	Acción	Resultado esperado
5	Revisar periódicamente	Inventario actualizado y accesos validados
6	Retirar o destruir	Baja documentada y eliminación segura

Este modelo no requiere comenzar con una estructura compleja. Lo importante es avanzar con criterio, priorizando los activos críticos. Una organización no debe intentar inventariar todo con el mismo nivel de detalle desde el primer día. Debe comenzar por aquello que afecta continuidad, cumplimiento, finanzas, clientes, datos personales y procesos críticos.

5 Políticas administrativas y gestión de accesos

La seguridad de la información no se sostiene únicamente sobre tecnología. Detrás de cada firewall, de cada sistema de autenticación, de cada control de acceso y de cada registro de auditoría existe un conjunto de políticas administrativas que determinan cómo deben comportarse las personas dentro de la organización respecto del acceso, uso y protección de la información.

Desde la administración de Tecnologías de Información, las políticas administrativas de seguridad son reglas formales que orientan conductas, asignan responsabilidades, establecen límites y permiten verificar cumplimiento. No son simples recomendaciones. Para que funcionen como controles reales, deben estar documentadas, aprobadas, comunicadas, aplicadas y auditadas.

Una política administrativa de seguridad cumple una función organizacional: traduce los riesgos tecnológicos en obligaciones concretas para directivos, empleados, contratistas, proveedores, áreas usuarias, Recursos Humanos, auditoría interna y el área de TI. Sin políticas claras, los controles técnicos pierden eficacia. Una contraseña robusta no alcanza si el usuario la anota en un papel visible. Un sistema de gestión de identidades no alcanza

si Recursos Humanos no informa una desvinculación. Un control de permisos no alcanza si los cambios de función no se comunican.

Para estudiantes de administración de empresas, este tema permite comprender que la seguridad de la información no es solo una cuestión de especialistas técnicos. Es una práctica de gestión que requiere coordinación, documentación, disciplina operativa y cultura organizacional.

Este material desarrolla las políticas administrativas básicas vinculadas con seguridad de información: escritorios limpios, pantallas bloqueadas, revocación de privilegios, ajuste de accesos por cambio de función, bloqueo por falta de uso, recertificación periódica, control de cuentas de servicio, documentación, comunicación, cultura y auditoría.

5.1 La política administrativa como instrumento de control

Una política de seguridad es una regla formal que indica qué conducta se espera, qué está permitido, qué está prohibido, quién es responsable y cómo se verificará el cumplimiento.

Una política escrita que nadie conoce, que no se aplica y cuyo incumplimiento no tiene consecuencias no es un control. Es solo un documento. Para convertirse en un control administrativo efectivo, debe integrarse al funcionamiento cotidiano de la organización.

Elemento	Función dentro de la política
Objetivo	Define qué riesgo busca reducir
Alcance	Indica a quiénes y a qué recursos se aplica
Responsables	Establece quién aprueba, ejecuta y controla
Reglas	Describe conductas obligatorias o prohibidas
Procedimiento	Explica cómo debe aplicarse
Evidencia	Define qué registros prueban cumplimiento
Consecuencias	Indica qué ocurre ante incumplimiento

Elemento	Función dentro de la política
Revisión	Establece periodicidad de actualización y auditoría

Ejemplo: una política de bloqueo de pantalla no debe limitarse a decir que "los usuarios deben bloquear sus equipos". Debe indicar tiempo máximo de inactividad, sistemas alcanzados, configuración técnica obligatoria, excepciones, responsables de implementación y forma de auditoría.

5.2 Atributos de una política efectiva

Una política administrativa de seguridad efectiva reúne cuatro atributos principales: documentación formal, comunicación, apoyo técnico y auditoría.

Atributo	Explicación	Ejemplo
Documentación formal	La política está escrita, aprobada y vigente	Política aprobada por dirección o comité correspondiente
Comunicación	Los usuarios conocen la regla y sus consecuencias	Capacitación inicial y recordatorios periódicos
Apoyo técnico	Los sistemas refuerzan la conducta esperada	Bloqueo automático de pantalla
Auditoría	Se verifica cumplimiento y se corrigen desvíos	Revisiones de accesos, inspecciones físicas o reportes

La política debe ser comprensible. Un documento excesivamente técnico puede ser difícil de aplicar. También debe ser proporcional. Una regla demasiado rígida puede generar atajos informales. Una regla demasiado laxa puede no reducir el riesgo.

La claridad es central. Una política debe permitir que una persona sepa qué debe hacer en una situación concreta.

5.3 Políticas administrativas y controles técnicos

Las políticas administrativas y los controles técnicos se complementan. La política define la regla. El control técnico ayuda a aplicarla. La auditoría verifica su cumplimiento.

Política administrativa	Control técnico de apoyo	Evidencia posible
Bloqueo de pantalla	Configuración automática por inactividad	Parámetros de GPO o configuración equivalente
Revocación de accesos	Desactivación centralizada de usuarios	Reporte de baja y estado de cuenta
Mínimo privilegio	Perfiles por rol	Matriz de permisos
Bloqueo por inactividad	Detección de último inicio de sesión	Reporte mensual de cuentas inactivas
Escritorio limpio	No siempre es técnico; requiere inspección	Actas de recorridas o checklist
Recertificación de accesos	Flujo de aprobación en sistema IAM	Confirmación del responsable funcional

Una política sin control técnico depende totalmente de la disciplina individual. Un control técnico sin política puede carecer de respaldo organizacional. La seguridad madura combina ambos elementos.

Ejemplo: la política establece que las pantallas deben bloquearse tras cinco minutos de inactividad en áreas con circulación externa. TI configura esa regla en los equipos. Auditoría verifica una muestra de estaciones de trabajo. La dirección respalda la política y aplica consecuencias si se incumple deliberadamente.

5.4 Política de escritorios limpios

La política de escritorios limpios establece que los espacios de trabajo físicos deben mantenerse libres de información sensible cuando no están siendo utilizados activamente.

Incluye documentos impresos, notas manuscritas, credenciales, dispositivos removibles, carpetas, formularios, contratos, listados, copias de reportes, apuntes con datos internos y cualquier soporte físico que contenga información de la organización.

Elemento expuesto	Riesgo	Conducta esperada
Documentos impresos	Lectura, fotografía o sustracción	Guardar bajo llave
Notas con datos sensibles	Exposición de información o claves	Eliminar o resguardar
Pendrives o discos externos	Pérdida o copia no autorizada	Guardar en lugar seguro
Credenciales físicas	Uso indebido de accesos	No dejarlas visibles
Contratos o reportes	Exposición de información estratégica	Archivar en repositorio seguro
Formularios con datos personales	Incumplimiento de confidencialidad	Custodiar y destruir correctamente

La regla no se limita al cierre de la jornada. También aplica durante ausencias breves, reuniones, pausas o traslados. En áreas donde circulan clientes, proveedores, personal de limpieza, técnicos externos o visitantes, la exposición física de información puede convertirse en una brecha de seguridad.

Ejemplo: un listado de clientes con correos y teléfonos queda sobre un escritorio durante una visita de un proveedor. Aunque no se produzca robo, la información puede ser fotografiada o leída. El riesgo surge por exposición física, no por falla técnica.

5.5 Pantallas bloqueadas

La política de escritorios limpios se extiende al entorno digital mediante la regla de pantallas bloqueadas. Toda computadora, notebook, tablet o dispositivo con sesión activa debe bloquearse cuando el usuario se ausenta.

Una pantalla desbloqueada con acceso a correo, sistemas de pagos, nómina, CRM, ERP o archivos compartidos representa un punto de acceso no autorizado. No requiere habilidades técnicas. Cualquier persona presente en el lugar puede consultar información o ejecutar acciones con la identidad del usuario.

Situación	Riesgo
Equipo desbloqueado con correo abierto	Lectura o envío de mensajes no autorizados
Sistema de pagos abierto	Operaciones indebidas
Nómina visible	Exposición de datos salariales
CRM abierto	Copia o consulta de datos de clientes
Carpeta compartida abierta	Eliminación, copia o modificación de archivos
Sesión administrativa abierta	Cambio de configuraciones críticas

El bloqueo puede ser manual o automático. El bloqueo automático debe configurarse desde TI para que no dependa únicamente de la disciplina del usuario. En áreas con circulación externa, el tiempo máximo de inactividad debería ser más corto. En áreas restringidas puede admitirse un período mayor, siempre proporcional al riesgo.

5.6 Implementación y verificación de escritorios limpios

La política de escritorios limpios requiere controles administrativos porque no todo puede verificarse técnicamente. Las inspecciones físicas permiten detectar documentos expuestos, soportes removibles, credenciales visibles o pantallas desbloqueadas.

Medio de verificación	Qué permite detectar
Recorridas físicas	Documentos o dispositivos visibles
Checklist de cumplimiento	Revisión sistemática por área
Pruebas controladas	Nivel de atención de los usuarios
Observación de pantallas	Sesiones abiertas sin supervisión
Reporte de incidentes	Casos detectados por compañeros o seguridad
Auditoría interna	Cumplimiento periódico de la política

La verificación no debe orientarse solo a sancionar. También debe permitir identificar fallas de comunicación, falta de capacitación, problemas de almacenamiento o ausencia de recursos. Si los empleados no tienen cajones, archivadores o destructoras disponibles, la política será más difícil de cumplir.

5.7 Gestión de identidades y ciclo de vida del acceso

La gestión de identidades administra el ciclo completo de vida de los usuarios y sus accesos. Este ciclo comienza con el alta, continúa con cambios de función, revisiones periódicas, bloqueo por inactividad y finaliza con la baja.

Etapa	Acción esperada
Alta	Crear usuario con permisos mínimos según función
Asignación inicial	Aprobar accesos por responsable funcional
Cambio de función	Retirar permisos anteriores y asignar nuevos
Proyecto temporal	Otorgar acceso con vencimiento

Etapa	Acción esperada
Licencia prolongada	Evaluar suspensión o restricción temporal
Inactividad	Bloquear cuentas sin uso legítimo
Baja	Revocar todos los accesos
Revisión periódica	Confirmar que los permisos siguen siendo necesarios

El objetivo es evitar que las cuentas queden activas sin necesidad, que los usuarios acumulen privilegios o que personas desvinculadas mantengan acceso a sistemas.

5.8 Revocación de privilegios ante la baja de usuarios

La revocación de accesos al momento de la baja es uno de los controles más importantes de seguridad administrativa. Un usuario dado de baja ya no tiene justificación para acceder a sistemas, datos, correo, redes, aplicaciones o instalaciones.

La baja puede producirse por renuncia, despido, finalización de contrato, jubilación, fallecimiento, vencimiento de una contratación externa o finalización de una beca. En todos los casos, el acceso debe retirarse en forma oportuna.

Acceso a revocar	Ejemplo
Directorio corporativo	Usuario de red o dominio
Correo electrónico	Cuenta corporativa
VPN	Acceso remoto
ERP o sistemas administrativos	Compras, ventas, contabilidad, nómina
CRM	Base de clientes y contactos
Plataformas en la nube	Documentos, repositorios y colaboración

Acceso a revocar	Ejemplo
Repositorios de código	Acceso a desarrollos
Tokens o claves API	Acceso programático
Credenciales físicas	Tarjetas de ingreso
Dispositivos	Notebooks, celulares o tokens físicos

Una baja parcial es un riesgo. Desactivar la cuenta principal, pero dejar activa la VPN, el correo, una plataforma externa o una tarjeta de acceso físico implica mantener puertas abiertas.

Ejemplo: una auditoría detecta cuentas activas de personas desvinculadas hace varios meses. La causa puede ser la falta de comunicación formal entre Recursos Humanos y TI. La corrección requiere bloquear accesos, investigar actividad posterior y establecer un procedimiento documentado.

5.9 Procedimiento de baja de accesos

El procedimiento de baja debe establecer quién inicia la solicitud, cuándo debe ejecutarse, qué sistemas se revisan, quién ejecuta el bloqueo, cómo se documenta y cómo se verifica.

Elemento del procedimiento	Criterio recomendado
Inicio	Recursos Humanos informa la desvinculación
Plazo	El mismo día de la baja; inmediato en casos conflictivos
Responsable técnico	TI ejecuta revocación en sistemas
Responsable funcional	Confirma accesos vinculados con el área
Alcance	Todos los sistemas, plataformas y credenciales
Evidencia	Ticket, registro de baja y reporte de cuentas

Elemento del procedimiento	Criterio recomendado
Verificación	Confirmación posterior de accesos revocados
Excepciones	Solo justificadas, aprobadas y temporales

En renuncias con preaviso, puede ser necesario mantener ciertos accesos durante la transición, pero deberían reducirse al mínimo necesario. En despidos conflictivos o desvinculaciones por motivos de seguridad, la revocación debe ser simultánea a la comunicación de la baja.

La verificación posterior es necesaria. No alcanza con iniciar el proceso. Debe confirmarse que los accesos fueron efectivamente revocados.

5.10 Ajuste de privilegios por cambio de función

Cuando una persona cambia de área, cargo, jerarquía o proyecto, sus necesidades de acceso cambian. Los permisos anteriores pueden dejar de ser necesarios y los nuevos permisos deben asignarse según la nueva función.

Si no se realiza esta revisión, aparece la acumulación gradual de privilegios. Una persona puede conservar accesos de puestos anteriores y sumar otros nuevos, hasta llegar a un perfil que ninguna función justifica.

Evento organizacional	Acción sobre accesos
Cambio de área	Retirar permisos del área anterior y asignar nuevos
Promoción	Revisar permisos operativos y de aprobación
Cambio lateral	Ajustar accesos a nuevas tareas
Asignación a proyecto	Otorgar permisos temporales
Fin de proyecto	Revocar permisos temporales

Evento organizacional	Acción sobre accesos
Regreso de licencia prolongada	Verificar vigencia de la función
Cambio de jefe o responsabilidades	Revisar accesos vinculados al proceso

Ejemplo: una persona que trabajaba en contabilidad pasa a auditoría interna. Si conserva permisos de escritura sobre el sistema contable y además recibe permisos de revisión, se genera una incompatibilidad. La función de auditoría requiere independencia respecto de los procesos auditados.

5.11 Principio de mínimo privilegio

El principio de mínimo privilegio indica que cada usuario debe contar solo con los accesos necesarios para cumplir su función actual. No debe conservar permisos por comodidad, antigüedad, jerarquía o costumbre.

Situación	Riesgo
Usuario con permisos de áreas anteriores	Acceso excesivo
Gerente con permisos operativos innecesarios	Posibilidad de alterar registros
Auditor con permisos de escritura	Falta de independencia
Proveedor con acceso permanente	Riesgo de tercero
Cuenta de proyecto sin vencimiento	Acceso olvidado
Permisos otorgados “por si acaso”	Superficie de ataque ampliada

El mínimo privilegio exige que cada permiso tenga justificación funcional. También exige revisiones periódicas, porque las funciones cambian.

5.12 Recertificación periódica de accesos

La recertificación de accesos es una revisión formal en la que cada responsable funcional confirma que los permisos de los usuarios de su área siguen siendo necesarios para la función actual.

No reemplaza el ajuste por cambio de función. Lo complementa. Sirve para detectar accesos acumulados, errores de asignación, cambios no informados o cuentas que no deberían seguir activas.

Elemento de recertificación	Descripción
Frecuencia	Trimestral o semestral para sistemas críticos
Responsable	Jefe o dueño funcional del proceso
Alcance	Usuarios, roles, perfiles y permisos críticos
Decisión	Confirmar, modificar o revocar
Evidencia	Registro de revisión y aprobación
Seguimiento	Revocación de accesos no confirmados

Ejemplo: el responsable de Tesorería recibe un listado de usuarios con permisos para aprobar pagos. Debe confirmar quiénes realmente necesitan ese permiso. Los accesos no confirmados deben revocarse.

La recertificación debe tener consecuencias. Si el responsable no confirma un acceso dentro del plazo, el sistema debe escalar el caso o suspender permisos sensibles.

5.13 Bloqueo de cuentas por falta de uso

Una cuenta sin uso durante un período prolongado representa un riesgo. Puede pertenecer a una persona en licencia, a un contratista finalizado, a un usuario que cambió de función o a un proyecto que nunca se completó. Si la cuenta sigue activa, puede ser utilizada sin que exista actividad legítima reciente que permita comparar comportamientos.

Tipo de cuenta inactiva	Riesgo
Empleado desvinculado no informado	Acceso no autorizado
Contratista finalizado	Acceso de tercero sin relación vigente
Usuario que cambió de función	Permiso innecesario
Cuenta de proyecto abandonado	Acceso olvidado
Cuenta anterior sin MFA	Mayor exposición
Cuenta con contraseña reutilizada	Riesgo por brechas externas

La política debe definir qué se considera inactividad. Para cuentas de usuarios comunes puede usarse un criterio de 30, 60 o 90 días, según el sistema. Para cuentas privilegiadas, el plazo debería ser más corto. La definición debe calibrarse según frecuencia de uso esperada.

5.14 Bloqueo versus eliminación

Bloquear una cuenta y eliminarla no son acciones equivalentes. El bloqueo impide el acceso, pero conserva la cuenta y sus configuraciones. La eliminación borra definitivamente la cuenta, según las reglas del sistema y las necesidades de evidencia.

Acción	Cuándo se aplica	Ventaja	Precaución
Bloqueo	Ante inactividad o revisión temporal	Evita acceso sin perder historial	Debe revisarse si corresponde reactivar o eliminar
Eliminación	Cuando ya no existe necesidad legítima	Reduce cuentas residuales	Debe preservar registros necesarios
Suspensión temporal	Licencia, proyecto pausado o investigación	Mantiene control durante un período	Requiere fecha de revisión

Acción	Cuándo se aplica	Ventaja	Precaución
Deshabilitación por baja	Desvinculación laboral o contractual	Cierra acceso	Debe abarcar todos los sistemas

La política puede definir dos umbrales: uno para bloqueo y otro para eliminación. Por ejemplo, cuenta bloqueada a los 60 días de inactividad y eliminada luego de un período adicional sin solicitud de reactivación.

La eliminación debe considerar obligaciones de auditoría. En ciertos sistemas puede ser preferible deshabilitar usuarios y conservar historial para no perder trazabilidad de operaciones pasadas.

5.15 Excepciones y reactivación de cuentas

No toda inactividad significa que la cuenta debe eliminarse de inmediato. Puede haber licencias prolongadas, asignaciones temporales, funciones estacionales o situaciones justificadas. Sin embargo, las excepciones deben ser formales.

Excepción posible	Documentación requerida
Licencia prolongada	Motivo, período estimado y responsable
Función estacional	Justificación y fecha de revisión
Proyecto pausado	Responsable del proyecto y vencimiento
Cuenta de auditoría	Finalidad, autorización y período
Soporte externo temporal	Contrato, responsable y fecha de expiración

La reactivación de una cuenta bloqueada por inactividad debe requerir aprobación del responsable funcional y verificación de que la persona sigue vinculada con la organización. No debería ser un proceso automático iniciado solo por el usuario.

5.16 Cuentas de servicio

Las cuentas de servicio son cuentas utilizadas por aplicaciones, tareas programadas, integraciones o procesos automatizados para interactuar con sistemas. No pertenecen a una persona individual, pero pueden tener permisos elevados.

Por esa razón, deben gestionarse con especial cuidado.

Riesgo en cuentas de servicio	Control recomendado
Permisos excesivos	Asignar solo permisos necesarios
Contraseñas sin rotación	Rotación controlada o credenciales administradas
Falta de responsable	Asignar dueño técnico y funcional
Cuenta sin uso	Revisar si el proceso sigue vigente
Uso compartido informal	Prohibir uso humano de cuentas de servicio
Falta de monitoreo	Registrar actividad y alertas
Integración abandonada	Deshabilitar cuenta si el sistema ya no opera

Una cuenta de servicio inactiva con permisos elevados representa un riesgo similar al de una cuenta de usuario inactiva. La diferencia es que su análisis requiere cuidado, porque la ausencia de actividad puede deberse a un proceso mensual, trimestral o eventual.

Cada cuenta de servicio debe tener responsable, finalidad, sistema asociado, permisos, frecuencia esperada de uso y fecha de revisión.

5.17 Integración de políticas en el ciclo completo del acceso

Las políticas descritas no operan de manera aislada. Forman un sistema integrado que gestiona el ciclo completo del acceso.

Etapa del ciclo	Política relacionada
Alta del usuario	Asignación inicial según función
Uso cotidiano	Escritorio limpio y pantalla bloqueada
Cambio de función	Ajuste de privilegios
Proyecto temporal	Acceso con vencimiento
Inactividad	Bloqueo de cuentas
Revisión periódica	Recertificación de accesos
Baja	Revocación completa de privilegios
Auditoría	Verificación de cumplimiento

Si falla una etapa, el sistema se debilita. Una organización puede revocar correctamente accesos al momento de la baja, pero si no gestiona cambios de función, acumulará usuarios con privilegios excesivos. Puede bloquear cuentas inactivas, pero si no controla escritorios y pantallas, seguirá exponiendo información en el entorno físico.

Ejemplo integrado: una organización reduce el tiempo promedio de revocación de accesos de varios días a pocas horas, bloquea cuentas inactivas, recertifica permisos críticos y mejora el cumplimiento de escritorios limpios. Esas métricas muestran madurez de control.

5.18 Documentación de las políticas

La documentación permite que las políticas sean conocidas, exigibles y auditables. Debe existir una versión vigente, aprobada y accesible para las personas alcanzadas.

Documento	Contenido esperado
Política formal	Regla general, alcance y responsabilidades

Documento	Contenido esperado
Procedimiento operativo	Pasos concretos para aplicar la política
Matriz de responsabilidades	Quién solicita, aprueba, ejecuta y controla
Registro de capacitación	Evidencia de comunicación
Formulario o ticket	Registro de solicitudes y aprobaciones
Reporte de auditoría	Resultado de revisiones
Plan de acción	Corrección de desvíos

La política debe actualizarse cuando cambian sistemas, riesgos, normativa, estructura organizacional o prácticas de trabajo. Una política desactualizada puede generar incumplimientos involuntarios o controles ineficaces.

5.19 Comunicación y capacitación

Las políticas administrativas no producen efectos si las personas no las conocen o no las entienden. La comunicación debe ser clara, periódica y adaptada al público.

Momento de comunicación	Contenido
Ingreso del empleado	Políticas básicas, uso aceptable, confidencialidad
Cambio de función	Nuevas responsabilidades y accesos
Implementación de política nueva	Alcance, fecha de vigencia y obligaciones
Recordatorio periódico	Reglas clave y errores frecuentes
Incidente relevante	Aprendizajes y acciones correctivas
Capacitación anual	Refuerzo general y evaluación

La capacitación debe explicar el motivo de la política. Una persona cumple mejor una regla cuando comprende el riesgo que reduce. Por ejemplo, no se trata solo de “ordenar

el escritorio", sino de evitar exposición de datos personales, información financiera o documentos confidenciales.

5.20 Cultura organizacional y liderazgo

La cultura de seguridad se construye con el tiempo. Requiere coherencia entre lo que la política establece y lo que los líderes practican. Si los directivos no cumplen las políticas, el resto de la organización percibe que las reglas son formales pero no reales.

Conducta de liderazgo	Efecto cultural
Cumplir escritorio limpio	Refuerza la regla
Bloquear pantalla en reuniones	Normaliza la práctica
Exigir baja oportuna de accesos	Prioriza seguridad
No solicitar excepciones injustificadas	Evita privilegios informales
Aceptar auditorías	Da legitimidad al control
Aplicar consecuencias de manera consistente	Mejora credibilidad

Las consecuencias del incumplimiento deben ser proporcionales y aplicarse de manera consistente. Aplicar sanciones solo a niveles operativos y no a niveles jerárquicos destruye la credibilidad del sistema de control.

5.21 Auditoría y métricas de cumplimiento

Las políticas deben medirse. Sin medición, la organización no sabe si las reglas se cumplen o si solo existen en documentos.

Métrica	Qué permite evaluar
Tiempo promedio de revocación de accesos	Oportunidad de bajas

Métrica	Qué permite evaluar
Cantidad de cuentas activas de ex empleados	Debilidad crítica
Cantidad de cuentas inactivas bloqueadas	Exposición reducida
Porcentaje de accesos recertificados	Madurez del control
Porcentaje de accesos no confirmados revocados	Efectividad de recertificación
Cumplimiento de escritorios limpios	Conducta física de seguridad
Pantallas desbloqueadas detectadas	Riesgo de acceso local
Excepciones activas	Riesgo aceptado y controlado
Cuentas de servicio revisadas	Control de accesos no personales
Incidentes por incumplimiento de política	Efectividad de capacitación

Ejemplo: si se detectan muchas cuentas inactivas en la primera revisión, puede ser un síntoma de falta de control histórico. Si en revisiones posteriores el número disminuye, puede observarse mejora. Si vuelve a crecer, debe revisarse el proceso de altas, bajas y cambios.

5.22 Matriz integradora de políticas administrativas

La siguiente matriz resume las políticas administrativas principales, el riesgo que reducen y la evidencia esperada.

Política	Riesgo que reduce	Evidencia
Escritorios limpios	Exposición física de información	Checklist, inspecciones y reportes

Política	Riesgo que reduce	Evidencia
Pantallas bloqueadas	Acceso local no autorizado	Configuración técnica y observaciones
Revocación por baja	Accesos de personas desvinculadas	Ticket de baja y reporte de bloqueo
Ajuste por cambio de función	Acumulación de privilegios	Solicitud, aprobación y revocación
Mínimo privilegio	Permisos excesivos	Matriz de roles
Recertificación	Accesos obsoletos	Confirmación del responsable
Bloqueo por inactividad	Cuentas olvidadas	Reporte de último acceso y bloqueo
Cuentas de servicio	Accesos no personales sin control	Inventario y revisión técnica
Comunicación	Desconocimiento de la política	Registro de capacitación
Auditoría	Falta de verificación	Informe y plan de acción

5.23 Síntesis del capítulo

Las políticas administrativas de seguridad de la información son un componente esencial del sistema de control organizacional. No reemplazan a los controles técnicos, pero permiten que esos controles funcionen dentro de un marco de responsabilidades, conductas esperadas y evidencias verificables.

La política de escritorios limpios y pantallas bloqueadas protege la información en el espacio físico y en las sesiones locales. La revocación de privilegios al momento de la baja cierra accesos de personas que ya no tienen relación con la organización. El ajuste

de privilegios por cambio de función mantiene el principio de mínimo privilegio a lo largo de la trayectoria laboral. La recertificación periódica permite detectar accesos que ya no corresponden. El bloqueo por inactividad reduce la exposición generada por cuentas sin uso legítimo. El control de cuentas de servicio evita que procesos automatizados se transformen en puertas de acceso no supervisadas.

Para estudiantes de administración de empresas, el aprendizaje central consiste en comprender que la seguridad de la información es una responsabilidad organizacional. La dirección aprueba y respalda las políticas. Recursos Humanos informa altas, cambios y bajas. TI implementa controles técnicos. Los responsables funcionales aprueban accesos. Auditoría verifica cumplimiento. Cada usuario cumple reglas en su trabajo cotidiano.

Cuando alguno de esos actores falla, el sistema de control se debilita. Por eso, una política de seguridad no debe evaluarse por su redacción, sino por su aplicación real, su evidencia, sus métricas y su capacidad para reducir riesgos.

6 Ingeniería social

6.1 La ingeniería social como riesgo de gestión

La **ingeniería social** (*Social Engineering*) es una forma de ataque basada en la manipulación de personas para obtener información, acceso a sistemas, autorización de operaciones, ejecución de pagos o entrega de credenciales. A diferencia de los ataques puramente técnicos, no comienza por explotar una falla de software: se apoya en decisiones humanas inducidas por **urgencia, confianza, temor, desconocimiento, presión jerárquica o rutina operativa**.

Desde la administración, este riesgo tiene una consecuencia importante: un sistema puede estar correctamente configurado y, aun así, la organización quedar expuesta si una persona entrega su contraseña, aprueba una solicitud falsa o permite el ingreso físico de un tercero no autorizado.

Un sistema de información (*Information System*, SI) está formado por **personas, procesos, datos y tecnología**. El usuario no es un elemento externo al sistema: sus

decisiones forman parte del funcionamiento real de los procesos digitales. Cuando un atacante manipula a un usuario autorizado, puede operar con credenciales válidas. Para el sistema, la acción parece legítima. Para la organización, puede ser el inicio de un fraude.

6.2 Modalidades de ataque

Las modalidades de ingeniería social varían según el canal utilizado, el objetivo del atacante y el nivel de personalización. Las más relevantes para organizaciones son las siguientes:

Modalidad	Canal	Descripción	Señal de alerta típica
Phishing	Correo electrónico o mensaje digital	Comunicación falsa que aparenta provenir de una fuente confiable para obtener credenciales, inducir descargas o forzar acciones	Dominio ligeramente diferente al real, urgencia inusual, enlace que no corresponde al remitente
Spear Phishing	Correo personalizado	Variante dirigida que usa datos reales del destinatario: su cargo, sus proveedores, sus procesos	Mencionan una factura real o un proveedor conocido; el nivel de detalle genera mayor confianza
Vishing	Llamada telefónica	El atacante se presenta como soporte técnico,	Solicitud de contraseña o código temporal por teléfono; presión

Modalidad	Canal	Descripción	Señal de alerta típica
		auditor, proveedor o autoridad interna	para actuar antes de cortar
Smishing	SMS o mensajería móvil	Incluye enlaces falsos, alertas de seguridad o instrucciones para instalar aplicaciones	Mensaje con URL acortada que redirige a un sitio falso
Pretexting	Cualquier canal	Construcción de una historia falsa (auditoría, urgencia de dirección, revisión de cuenta) para que la víctima actúe sin verificar	Contexto elaborado que no puede confirmarse por los canales habituales
Baiting	Digital o físico	Ofrece algo atractivo (archivo, descarga, dispositivo) para inducir una conducta insegura	Dispositivo USB abandonado; archivo "confidencial" adjunto no solicitado
Tailgating	Físico	Persona no autorizada ingresa a un área restringida	Persona sin credencial que ingresa detrás de un

Modalidad	Canal	Descripción	Señal de alerta típica
		siguiendo a alguien con acceso legítimo	empleado sin que nadie lo cuestione
Quid pro quo	Cualquier canal	El atacante ofrece asistencia o una ventaja a cambio de información o acceso	"Te ayudo a resolver el problema si me pasás tu usuario"
Dumpster Diving	Físico / digital	Obtiene información de documentos descartados, dispositivos obsoletos o soportes eliminados sin proceso seguro	Listados, contraseñas escritas o etiquetas en papeles desechados

6.3 Factores que aumentan la exposición organizacional

La ingeniería social no prospera solo por errores individuales. Encuentra oportunidades en debilidades de diseño organizacional.

Factor de exposición	Por qué genera riesgo	Ejemplo
Procedimientos informales o no verificables	Una solicitud puede procesarse sin confirmar quién la hizo ni por qué	Modificar datos bancarios de un proveedor solo con base en un correo

Factor de exposición	Por qué genera riesgo	Ejemplo
Concentración de funciones	Una sola persona puede crear, modificar y aprobar sin control cruzado	El mismo empleado crea un proveedor, cambia su cuenta y aprueba el pago
Exceso de permisos	Si una cuenta es comprometida, el daño es proporcional a sus permisos	Un usuario con acceso de administrador permite al atacante operar sin restricciones
Ausencia de capacitación	Los empleados no reconocen señales de alerta ni saben cómo reportar	Nadie advierte que el dominio del remitente tiene una letra cambiada
Falta de monitoreo	La organización puede detectar tarde o nunca que ocurrió un incidente	Sin registros de auditoría, no es posible reconstruir qué cambió, cuándo y quién

El problema no siempre está en el usuario. Con frecuencia está en el diseño del control que permite actuar sin verificar.

6.4 Impacto en la organización

El impacto de un ataque de ingeniería social se extiende a múltiples dimensiones:

Dimensión	Descripción	Ejemplo concreto
Económico	Transferencias fraudulentas, pagos duplicados, desvío de fondos, costos de recuperación técnica y	Un cambio de CBU genera pérdida de dos o tres pagos mensuales al proveedor falso y mantiene la deuda con el proveedor real

Dimensión	Descripción	Ejemplo concreto
	legal, horas internas de investigación	
Operativo	Bloqueo de cuentas, suspensión de servicios, detención de pagos, interrupción de facturación, activación de planes de contingencia	Si el incidente afecta el ERP, puede alcanzar compras, ventas, inventario, contabilidad y tesorería simultáneamente
Sobre la información (tríada CIA)	Pérdida de confidencialidad (robo de datos), integridad (modificación de registros) o disponibilidad (bloqueo de cuentas o instalación de malware)	Un atacante con acceso a credenciales puede exportar la base de clientes, modificar precios o instalar un ransomware
Legal y regulatorio	Obligaciones de investigación, preservación de evidencia, notificación a afectados, revisión de contratos, exposición a reclamos	El compromiso de datos personales puede generar sanciones regulatorias y litigios que emergen meses después del incidente
Reputacional	Pérdida de confianza en clientes, proveedores, empleados y socios comerciales	En servicios profesionales, salud, finanzas o comercio electrónico, la confianza forma parte del valor organizacional

6.5 Matriz de riesgo aplicada a ingeniería social

La matriz combina **probabilidad** e **impacto** para priorizar qué riesgos requieren atención urgente.

Nivel de riesgo = Probabilidad × Impacto

6.5.1 Escala de valoración

Valor	Probabilidad	Criterio	Impacto	Criterio en TI y administración
1	Muy baja	Caso excepcional	Muy bajo	No afecta procesos relevantes ni datos sensibles
2	Baja	Sin antecedentes recientes	Bajo	Afecta pocos usuarios; se corrige sin interrupción relevante
3	Media	Puede ocurrir en el año	Medio	Genera demoras, reprocesos o exposición limitada
4	Alta	Probable sin controles	Alto	Afecta pagos, clientes, datos personales o cumplimiento

Valor	Probabilidad	Criterio	Impacto	Criterio en TI y administración
5	Muy alta	Se espera con frecuencia	Muy alto	Produce fraude, filtración grave, pérdida económica o interrupción crítica

6.5.2 Escenarios evaluados

Riesgo	Prob.	Impacto	Nivel	Clasificación	Tratamiento sugerido
Phishing masivo a empleados administrativos	4	4	**16**	Alto	Filtros de correo, capacitación, MFA y reportes internos
Spear phishing al área de pagos	3	5	**15**	Alto	Doble validación, control de cambios bancarios, segregación de funciones

Riesgo	Prob.	Impacto	Nivel	Clasificación	Tratamiento sugerido
Vishing a mesa de ayuda para restablecer claves	3	4	**12**	Alto	Verificación formal de identidad y registro de solicitudes
Falso soporte técnico solicitando datos	3	4	**12**	Alto	Canales oficiales, prohibición de compartir claves y auditoría
Smishing a teléfonos corporativos	3	3	**9**	Medio	Capacitación, control de enlaces y política de uso móvil
Tailgating en oficinas con documentación sensible	2	4	**8**	Medio	Control de ingreso, credenciales visibles y registro de visitantes
Baiting mediante	2	4	**8**	Medio	Bloqueo de puertos USB,

Riesgo	Prob.	Impacto	Nivel	Clasificación	Tratamiento sugerido
dispositivo externo					control de dispositivos y capacitación
Descarte inseguro de documentación	2	3	**6**	Medio	Destrucción segura y política de escritorio limpio

La matriz debe revisarse con datos reales: incidentes previos, cantidad de cuentas privilegiadas, nivel de capacitación, dependencia del correo electrónico y calidad de los controles existentes.

6.6 Controles recomendados

La reducción del riesgo de ingeniería social exige un enfoque combinado. Los controles técnicos son necesarios pero no suficientes: deben acompañarse de procedimientos administrativos y reglas de decisión.

6.6.1 Controles técnicos y administrativos

Control	Qué hace	Dónde aplica prioritariamente
MFA (*Multi-Factor Authentication*)	Requiere más de un factor para ingresar a sistemas; reduce el daño cuando una contraseña es robada	Correo corporativo, sistemas administrativos, accesos remotos, cuentas privilegiadas

Control	Qué hace	Dónde aplica prioritariamente
Gestión de accesos (*Access Management*)	Controla altas, bajas y modificaciones de usuarios con autorización formal y revisión periódica	Todos los sistemas con datos sensibles; revocación inmediata ante desvinculación o cambio de función
Segregación de funciones (SoD)	Separa tareas incompatibles para evitar que una sola persona controle todo el circuito	Pagos: una persona carga la factura, otra la aprueba, otra ejecuta el pago
Verificación por canal independiente	Toda solicitud sensible se valida por un medio diferente al que la originó	Cambios de datos bancarios, pedidos de urgencia, solicitudes fuera de procedimiento
Registros de auditoría (*Audit Logs*)	Documentan accesos, cambios, aprobaciones e intentos fallidos; permiten detectar anomalías	Sistemas de pagos, ERP, correo corporativo, bases de datos de clientes
Capacitación y simulaciones	Formación breve, periódica y orientada a casos reales; las simulaciones miden exposición real	Todos los empleados con acceso a sistemas o información sensible
Política de escritorio limpio (*Clean Desk Policy*)	Prohíbe dejar documentos, contraseñas o dispositivos visibles sin custodia;	Áreas con documentación física: administración, RR.HH., finanzas, legal

Control	Qué hace	Dónde aplica prioritariamente
	complementa con destrucción segura	
Control de dispositivos externos	Limita uso de memorias USB y equipos no autorizados; puede incluir bloqueo técnico de puertos	Equipos corporativos de producción; áreas con información sensible
Canales oficiales de soporte	Todo pedido de soporte ingresa por canales definidos con trazabilidad	Mesa de ayuda, restablecimiento de contraseñas, acceso remoto
Plan de respuesta a incidentes (IRP)	Define detección, contención, análisis, comunicación, recuperación y lecciones aprendidas	Toda la organización; con responsables y tiempos máximos definidos

6.6.2 Verificación por canal independiente — El control más subestimado

Este control merece atención especial porque cubre el punto más explotado por la ingeniería social: la confianza en el canal original.

Situación	Práctica incorrecta	Práctica correcta
Llega un correo pidiendo cambiar el CBU de un proveedor	Se procesa el cambio respondiendo el mismo correo	Se llama al contacto registrado previamente del proveedor para confirmar

Situación	Práctica incorrecta	Práctica correcta
Llega un pedido de transferencia urgente del "CEO" por email	Se aprueba la transferencia por la urgencia aparente	Se confirma por teléfono con el directivo usando el número corporativo, no el del correo
Mesa de ayuda recibe llamada para restablecer contraseña	Se procede sin verificar identidad del solicitante	Se exige validación por el sistema de tickets y confirmación por canal secundario

Si llega un correo con un cambio bancario, la validación nunca debe hacerse respondiendo ese mismo mensaje.

6.7 Indicadores para la gestión del riesgo

Los indicadores permiten medir si el riesgo disminuye, se mantiene o aumenta con el tiempo. Deben presentarse de forma comprensible para la dirección.

Indicador	Qué mide	Cómo interpretarlo
Tasa de clics en simulaciones	Porcentaje de usuarios que hacen clic en enlaces de prueba	El 14% indica necesidad de refuerzo si el objetivo es menor al 5%
Tasa de reporte	Porcentaje de usuarios que informan mensajes sospechosos	Una tasa del 40% puede indicar mejor detección temprana
Tiempo promedio de reporte	Tiempo entre recepción del mensaje y aviso interno	Reportes en menos de 15 minutos facilitan el bloqueo preventivo

Indicador	Qué mide	Cómo interpretarlo
Cuentas sin MFA	Usuarios sin segundo factor de autenticación	Debe tender a 0 en sistemas críticos
Cambios bancarios sin doble validación	Excepciones al procedimiento de pagos	Debe ser 0 en proveedores activos
Usuarios con permisos excesivos	Cuentas con accesos no justificados por su función	Revisión mensual en áreas críticas
Solicitudes de soporte fuera de canal	Pedidos recibidos por medios no autorizados	Ayuda a corregir hábitos internos
Documentos sensibles descartados sin control	Hallazgos en revisiones internas	Debe activar medidas de destrucción segura y capacitación

Un tablero trimestral puede incluir: cantidad de incidentes, áreas afectadas, tipo de ataque, tiempo de respuesta, controles pendientes y evolución de la capacitación. En áreas críticas, la revisión mensual es más adecuada.

6.8 Responsabilidades de la administración

La ingeniería social no se gestiona solo con tecnología. La administración debe intervenir diseñando procesos menos vulnerables, con reglas claras, evidencia verificable y capacidad de respuesta ante incidentes.

Acción	Descripción
Identificar procesos críticos	Pagos, altas de proveedores, gestión de usuarios, atención al cliente y contratación de servicios son áreas de alta exposición
Documentar controles	Una regla informal no es suficiente: debe existir un procedimiento con

Acción	Descripción
	responsables, evidencias y criterios de excepción
Revisar permisos	Los accesos deben corresponderse con funciones reales; los permisos acumulados por cambios de puesto generan exposición innecesaria
Exigir trazabilidad	Las operaciones sensibles deben dejar evidencia: quién solicitó, quién aprobó, qué se modificó y cuándo
Tratar la capacitación como control permanente	Un curso aislado no alcanza; la formación debe repetirse, actualizarse y medirse con indicadores
Integrar a proveedores	Los contratos deben incluir validación de identidad, notificación de incidentes, confidencialidad y mecanismos de verificación
Preparar la respuesta	Definir qué hacer cuando ocurre un incidente; un reporte temprano puede reducir daños de forma significativa

7 Seguridad de los datos

La seguridad de datos comprende el conjunto de criterios, controles y procedimientos destinados a proteger la información durante todo su ciclo de vida: creación, captura, almacenamiento, procesamiento, transmisión, consulta, archivo y eliminación.

Desde la administración de Tecnologías de la Información, los datos son el insumo básico de los sistemas de información. Sin datos confiables, los sistemas pierden valor

administrativo, contable, operativo y estratégico. Una organización puede contar con aplicaciones modernas, reportes visuales y tableros automatizados, pero si los datos son incorrectos, incompletos o inaccesibles, las decisiones resultantes serán débiles.

En una organización, los datos permiten facturar, cobrar, pagar, controlar inventarios, liquidar sueldos, atender clientes, cumplir obligaciones legales, elaborar presupuestos, tomar decisiones y evaluar resultados. Por ello, su seguridad no puede reducirse a impedir accesos indebidos. También debe asegurar que los datos sean correctos, completos, oportunos, disponibles, trazables y útiles para el proceso de negocio que los utiliza.

Los tres pilares tradicionales de la seguridad de datos son confidencialidad, integridad y disponibilidad. Estos conceptos forman la triada CIA, por sus siglas en inglés: *Confidentiality, Integrity and Availability*.

Pilar	Pregunta central	Ejemplo administrativo
Confidencialidad	¿Quién puede acceder al dato?	Solo Recursos Humanos puede consultar legajos del personal.
Integridad	¿El dato es correcto y no fue alterado indebidamente?	Una cuenta bancaria de proveedor no puede modificarse sin aprobación.
Disponibilidad	¿El dato está accesible cuando se necesita?	El sistema de facturación debe estar operativo durante el horario comercial.

Junto con estos pilares aparecen otros conceptos relevantes para la administración: accesibilidad, validación, controles de entrada, controles de proceso, controles de salida, pistas de auditoría, integridad de mensajes, calidad de datos, gobierno de datos y

minimización. Todos estos elementos permiten que la información sea segura, útil y controlable.

7.1 Seguridad de datos como función organizacional

La seguridad de datos debe entenderse como una responsabilidad de toda la organización. El área de Tecnologías de la Información administra plataformas, permisos, bases de datos, respaldos, integraciones, registros y herramientas de protección. Sin embargo, las áreas usuarias definen qué datos se necesitan, qué significan, cómo se cargan, quién los aprueba, cómo se corrigen y qué impacto tiene un error.

Un dato puede ser técnicamente válido y administrativamente incorrecto. Por ejemplo, un sistema puede aceptar una fecha con formato correcto, pero esa fecha puede no corresponder al contrato real. También puede aceptar un número de cuenta bancaria con longitud válida, aunque pertenezca a otro proveedor. Por eso, la seguridad de datos no se agota en validaciones técnicas. Necesita controles de negocio.

La administración debe asignar responsables sobre los datos críticos.

Rol	Responsabilidad principal	Ejemplo
Dueño del dato	Define reglas de uso, calidad, acceso y conservación	El área de Compras define datos comerciales de proveedores.
Custodio del dato	Implementa medidas técnicas de almacenamiento, respaldo y protección	TI administra la base de datos y sus permisos.
Usuario autorizado	Usa el dato según su función	Tesorería consulta datos bancarios para pagos.

Rol	Responsabilidad principal	Ejemplo
Auditor	Revisa evidencias, accesos, cambios y controles	Auditoría verifica modificaciones de datos críticos.

Ejemplo: en una base de proveedores, Compras puede ser responsable funcional de datos comerciales. Tesorería puede ser responsable de los datos bancarios. TI administra el sistema. Auditoría revisa evidencias. Esta distribución reduce errores y mejora la trazabilidad.

7.2 Confidencialidad y acceso autorizado

La confidencialidad exige que los datos solo estén disponibles para personas, procesos o sistemas autorizados. En administración, esto se vincula con legajos, sueldos, datos de clientes, contratos, estados financieros, información tributaria, claves, reportes internos y documentación legal.

El acceso debe basarse en necesidad funcional. Una persona no debería acceder a información solo por jerarquía, comodidad o costumbre. Debe existir una razón operativa. El principio de mínimo privilegio indica que cada usuario debe tener el nivel de acceso indispensable para cumplir su tarea.

Situación	Riesgo	Control recomendado
Usuario con acceso a datos que no necesita	Exposición innecesaria de información	Revisión de permisos y mínimo privilegio
Descarga masiva de una base sensible	Fuga de información	Restricción de exportación y monitoreo
Cuenta compartida	Falta de trazabilidad	Usuarios individuales
Acceso remoto sin protección	Ingreso indebido	Autenticación multifactor y VPN

Situación	Riesgo	Control recomendado
Datos sensibles sin cifrado	Exposición ante pérdida o robo	Cifrado en almacenamiento y transmisión

Los accesos se administran mediante identificación, autenticación y autorización. La identificación declara quién es el usuario. La autenticación verifica esa identidad. La autorización define qué puede hacer. Para datos sensibles, conviene utilizar autenticación multifactor, revisión periódica de permisos y registros de consulta.

Ejemplo: un usuario de ventas puede necesitar consultar datos de clientes, pero no descargar toda la base. Un usuario de Recursos Humanos puede consultar legajos, pero no modificar datos salariales sin aprobación. Un responsable de Tesorería puede ver cuentas bancarias de proveedores, pero los cambios deberían requerir doble validación.

7.3 Integridad de datos

La integridad de datos implica que la información sea exacta, completa y no haya sido modificada de manera indebida. Puede afectarse por errores de carga, fallas de software, cambios no autorizados, integraciones defectuosas, importaciones masivas mal configuradas, problemas de conversión o manipulación intencional.

En sistemas administrativos, la integridad es crítica. Un importe mal registrado puede afectar la facturación. Una cantidad de stock incorrecta puede generar ventas imposibles de cumplir. Un CBU erróneo puede dirigir un pago a una cuenta equivocada. Un dato fiscal incorrecto puede impactar en impuestos, retenciones y obligaciones contables.

Dato afectado	Consecuencia administrativa posible
Precio de venta	Facturación incorrecta o pérdida comercial
Stock disponible	Compromisos de entrega imposibles de cumplir
Cuenta bancaria de proveedor	Pago indebido o fraude

Dato afectado	Consecuencia administrativa posible
Categoría fiscal	Retenciones o impuestos mal calculados
Legajo de empleado	Liquidación salarial incorrecta
Saldo contable	Estados financieros distorsionados

La integridad requiere controles preventivos y detectivos. Entre los preventivos se encuentran validaciones, permisos, segregación de funciones, autorizaciones, límites por monto y reglas de negocio. Entre los detectivos se encuentran conciliaciones, reportes de excepción, totales de control, controles cruzados y pistas de auditoría.

Ejemplo: un sistema de pagos puede impedir que una persona cargue y apruebe la misma transferencia. También puede registrar todo cambio de cuenta bancaria, exigir documentación, enviar alerta al responsable y requerir aprobación de una segunda persona. Estos controles protegen la integridad de los datos y reducen el riesgo de fraude.

7.4 Disponibilidad y accesibilidad

La disponibilidad indica que los datos estén accesibles cuando se necesitan. La accesibilidad agrega una dimensión práctica: los datos deben poder usarse por personas autorizadas de manera comprensible, oportuna y compatible con el proceso.

Una base de datos puede estar disponible técnicamente, pero ser inaccesible para el área usuaria si no hay permisos correctos, si la consulta tarda demasiado o si el formato no permite análisis. Por eso, disponibilidad y accesibilidad deben evaluarse en conjunto.

Concepto	Significado	Ejemplo
Disponibilidad técnica	El sistema o base de datos funciona	El servidor está activo.
Accesibilidad funcional	El usuario autorizado puede usar el dato	El área de ventas puede consultar clientes en tiempo útil.

Concepto	Significado	Ejemplo
Oportunidad	El dato está disponible en el momento necesario	El reporte de cobranzas se emite antes del cierre diario.
Usabilidad	El dato se presenta en formato comprensible	El tablero muestra información clara y exportable.

La disponibilidad depende de infraestructura, aplicaciones, comunicaciones, respaldos, bases de datos, soporte y continuidad operativa. Una interrupción de dos horas puede ser tolerable para un archivo histórico, pero grave para un sistema de facturación. Por eso, los datos deben clasificarse según criticidad.

Indicadores útiles son RTO y RPO. El RTO define cuánto tiempo puede estar caído un servicio. El RPO define cuánta información puede perderse medida en tiempo. Si el sistema de ventas tiene RTO de cuatro horas y RPO de una hora, la arquitectura de respaldo y recuperación debe cumplir esos límites.

7.5 Validación de datos

La validación de datos verifica que la información ingresada o procesada cumpla condiciones definidas. Puede revisar formato, tipo, longitud, rango, obligatoriedad, consistencia, duplicidad, relación con otros datos y reglas del negocio.

Tipo de validación	Qué controla	Ejemplo
Formato	Que el dato tenga una forma válida	Fecha con formato día/mes/año
Tipo	Que el dato sea numérico, texto, fecha u otro tipo esperado	Importe expresado como número

Tipo de validación	Qué controla	Ejemplo
Longitud	Que el dato tenga cantidad esperada de caracteres	Identificador fiscal con cantidad válida de dígitos
Rango	Que el dato esté dentro de límites permitidos	Descuento menor o igual al máximo autorizado
Obligatoriedad	Que el campo no quede vacío	Proveedor obligatorio en una factura
Duplicidad	Que no exista un registro repetido	Factura ya cargada
Consistencia	Que el dato no contradiga otros	Fecha de baja posterior a fecha de ingreso
Regla de negocio	Que el dato cumpla condiciones administrativas	Cuenta contable compatible con el tipo de comprobante

La validación debe aplicarse en capas. Puede existir en la interfaz de usuario, en la aplicación, en la base de datos y en procesos de revisión. Si una validación solo existe en la pantalla, una importación masiva podría evitarla. Si existe también en la base de datos, el control es más resistente.

Ejemplo: para cargar proveedores, el sistema puede validar CUIT o identificador fiscal, razón social, tipo de proveedor, cuenta bancaria, condición tributaria y documentación adjunta. Si falta un dato crítico, no debería permitir activar el proveedor para pagos.

7.6 Controles de entrada

Los controles de entrada buscan asegurar que la información capturada sea completa, autorizada, válida y oportuna. Son relevantes porque muchos errores administrativos comienzan en la carga inicial. Si el dato ingresa mal, todo proceso posterior puede quedar afectado.

Control de entrada	Función	Ejemplo
Campo obligatorio	Impide cargas incompletas	No permite grabar una factura sin proveedor.
Máscara de entrada	Define formato	Fecha, CUIT, código postal o número de cuenta.
Lista desplegable	Reduce escritura libre y variaciones	Provincias, categorías o centros de costo.
Validación de duplicados	Evita registros repetidos	Factura con mismo proveedor, tipo y número.
Límite de rango	Impide valores fuera de regla	Descuento superior al autorizado.
Formulario prenumerado	Permite detectar faltantes o duplicados	Solicitudes o comprobantes con numeración correlativa.
Control de lote	Compara cantidad e importe total	Lote de facturas ingresadas contra documentación recibida.
Revisión por supervisor	Agrega control humano	Validación de altas de proveedores.

Ejemplo: en la carga de facturas, el sistema puede exigir número de comprobante, fecha, proveedor, importe, impuesto, centro de costo y aprobación. También puede impedir duplicados por combinación de proveedor, tipo y número de comprobante. Si se detecta duplicado, debe generar alerta antes de continuar.

7.7 Controles de proceso

Los controles de proceso verifican que los datos sean tratados en forma completa, exacta y autorizada durante cálculos, transformaciones, actualizaciones, integraciones, importaciones, exportaciones y procesos automáticos.

En sistemas administrativos, los controles de proceso son esenciales. Una liquidación de sueldos, una actualización de precios, una conciliación automática, una importación bancaria o una asignación de stock pueden generar cientos o miles de movimientos. Si el proceso falla, el impacto se multiplica.

Control de proceso	Finalidad	Ejemplo
Total de control	Verifica importes o cantidades esperadas	Total del archivo de cobranzas antes y después de importar.
Conteo de registros	Detecta faltantes o duplicados	El archivo tenía 3.000 registros y se importaron 2.997.
Conciliación entre módulos	Compara información de sistemas distintos	Ventas contra contabilidad.
Validación de secuencia	Detecta saltos o duplicados	Numeración de facturas o recibos.
Revisión de excepciones	Enfoca casos fuera de regla	Pagos rechazados o importes superiores al límite.
Bloqueo durante procesamiento	Evita cambios simultáneos	Cierre de nómina mientras se liquida.

Control de proceso	Finalidad	Ejemplo
Bitácora de ejecución	Registra proceso, usuario, fecha y resultado	Proceso masivo ejecutado por un operador.
Prueba previa	Reduce fallas en producción	Ensayo de actualización de precios en ambiente separado.

Ejemplo: antes de importar 3.000 cobranzas, el sistema puede calcular cantidad de registros, importe total y fecha del archivo. Luego de importar, debe comparar resultados. Si el archivo tenía 3.000 registros por 15.000.000 de pesos y el sistema incorporó 2.997 registros por 14.850.000 pesos, debe informar la diferencia y bloquear el cierre automático hasta su revisión.

7.8 Controles de salida

Los controles de salida buscan asegurar que la información producida sea completa, correcta, autorizada, protegida y entregada al destinatario adecuado. Una salida puede ser un reporte, una factura, una orden de pago, un archivo bancario, una liquidación, un tablero de indicadores o una exportación de datos.

El riesgo de salida es relevante porque los datos procesados suelen circular fuera del sistema. Un reporte enviado al destinatario equivocado puede exponer información. Un archivo bancario mal generado puede producir pagos incorrectos. Un tablero con datos incompletos puede llevar a decisiones equivocadas.

Control de salida	Riesgo que reduce	Ejemplo
Revisión de destinatarios	Envío a persona equivocada	Validar destinatarios antes de enviar nómina.
Clasificación del reporte	Uso indebido de información	Marcar reporte como confidencial.

Control de salida	Riesgo que reduce	Ejemplo
Permisos de descarga	Extracción masiva no autorizada	Solo ciertos perfiles pueden exportar bases.
Cifrado de archivos	Lectura no autorizada	Archivo de pagos protegido.
Total de control	Salida incompleta o alterada	Importe total del archivo bancario.
Aprobación previa	Emisión sin autorización	Revisión de orden de pago antes de enviar.
Registro de emisión	Falta de trazabilidad	Usuario, fecha, reporte y destinatario.
Conservación de versiones	Confusión entre documentos	Identificar versión vigente del reporte.

Ejemplo: antes de enviar un archivo de pagos, el sistema puede mostrar cantidad de operaciones, importe total, cuentas destino y responsable aprobador. Luego puede requerir confirmación de una segunda persona. Después del envío, la conciliación bancaria verifica que lo ejecutado coincida con lo autorizado.

7.9 Pistas de auditoría

Las pistas de auditoría son registros que permiten reconstruir operaciones. Permiten saber quién hizo qué, cuándo, desde dónde, sobre qué registro y con qué resultado. En operaciones sensibles, también deberían registrar valor anterior y valor nuevo.

Sin pistas de auditoría, la organización pierde capacidad de investigación. Puede saber que un dato cambió, pero no quién lo cambió ni cuándo. Esto afecta control interno, responsabilidad, auditoría y respuesta ante incidentes.

Dato de auditoría	Utilidad
Usuario	Identifica quién ejecutó la acción.
Fecha y hora	Permite reconstruir la secuencia temporal.
Terminal o dirección de origen	Ayuda a ubicar desde dónde se operó.
Operación realizada	Describe la acción ejecutada.
Registro afectado	Indica qué dato fue modificado o consultado.
Valor anterior	Permite conocer el estado previo.
Valor nuevo	Permite conocer el cambio realizado.
Motivo o referencia	Aporta justificación documental.
Aprobación asociada	Vincula el cambio con una autorización.

Ejemplo: si se modifica la cuenta bancaria de un proveedor, la pista de auditoría debería registrar usuario, fecha, hora, dato anterior, dato nuevo, motivo, documento adjunto y aprobación. Si luego se produce un pago indebido, esa información permite reconstruir el circuito.

Una pista de auditoría útil debe ser completa, protegida contra alteración, consultable por personal autorizado y conservada durante un plazo definido. También debe evitar registrar información sensible innecesaria.

7.10 Integridad de mensajes

La integridad de mensajes busca asegurar que una comunicación, archivo o transacción no haya sido alterada durante su transmisión. Es relevante en pagos, intercambio de archivos, comunicaciones entre sistemas, órdenes de compra, facturación electrónica, transferencias de datos e interfaces de programación.

Una forma de verificar integridad es utilizar hash, es decir, una huella digital calculada sobre un conjunto de datos. Si el contenido cambia, el hash cambia. También pueden utilizarse firmas digitales o mecanismos criptográficos que permiten verificar origen e integridad.

Mecanismo	Qué permite verificar	Ejemplo
Hash	Que el contenido no cambió	Comparar archivo antes y después de enviarlo.
Firma digital	Origen e integridad del documento	Validar una orden electrónica.
Cifrado de comunicación	Confidencialidad durante transmisión	Enviar datos por canal seguro.
Control de secuencia	Que no falten mensajes	Verificar numeración de transacciones.
Acuse de recibo	Que el destinatario recibió el mensaje	Confirmación de recepción de archivo bancario.

Ejemplo: una organización genera un archivo de pagos. Antes de enviarlo, calcula un hash y registra el valor. Al recibirlo o procesarlo, se recalcula. Si el resultado no coincide, el archivo fue alterado o dañado. El proceso debe detenerse hasta aclarar la diferencia.

La integridad de mensajes no solo protege contra ataques. También detecta errores técnicos, corrupción de archivos, transferencias incompletas o fallas de integración.

7.11 Calidad de datos

La calidad de datos es la aptitud de los datos para su uso previsto. Un dato puede estar protegido contra accesos indebidos y, aun así, ser inútil si es incompleto, duplicado, inconsistente, desactualizado o incorrecto.

Dimensión de calidad	Significado	Ejemplo
Exactitud	Representa correctamente la realidad	La dirección registrada coincide con la real.
Completitud	No faltan datos necesarios	El proveedor tiene datos fiscales y bancarios completos.
Consistencia	No contradice otros datos	El saldo del módulo de ventas coincide con contabilidad.
Oportunidad	Está actualizado para el uso previsto	El stock refleja movimientos recientes.
Unicidad	No existen duplicados indebidos	Un cliente no figura cargado tres veces.
Validez	Cumple reglas definidas	El identificador fiscal tiene formato correcto.

Ejemplo: una base de clientes con direcciones desactualizadas afecta entregas y cobranzas. Una base de proveedores duplicada puede generar pagos repetidos. Un inventario inconsistente entre sistema y depósito puede producir ventas sin stock. Un reporte financiero con datos incompletos puede distorsionar decisiones.

La calidad debe medirse. Indicadores útiles pueden ser porcentaje de registros incompletos, cantidad de duplicados, antigüedad promedio de actualización, cantidad de errores por lote, diferencias entre sistemas y reclamos por datos incorrectos.

7.12 GIGO: Garbage In, Garbage Out

GIGO significa *Garbage In, Garbage Out*, expresión que puede traducirse como “basura entra, basura sale”. Resume una regla básica de los sistemas de información: si los datos de entrada son malos, el resultado será malo, aunque el sistema procese correctamente.

Este principio es especialmente importante para administración. Los sistemas no corrigen por sí solos la falta de control sobre la captura de datos. Si se carga mal un precio, el sistema puede facturar mal. Si se registra mal una condición fiscal, puede calcular retenciones equivocadas. Si se ingresa mal el stock, puede generar compras innecesarias o incumplimientos de entrega.

GIGO también afecta reportes, indicadores y modelos analíticos. Un tablero de gestión con datos duplicados o incompletos puede mostrar resultados aparentemente precisos, pero falsos. La exactitud visual de un gráfico no garantiza la calidad del dato.

Situación	Consecuencia
Precio cargado incorrectamente	Facturación errónea
Stock mal registrado	Ventas imposibles de cumplir
Proveedor duplicado	Pagos repetidos
Cliente mal clasificado	Reportes comerciales distorsionados
Datos históricos incompletos	Proyecciones poco confiables

Ejemplo: un informe muestra que una sucursal vendió 20% más que el mes anterior. Luego se detecta que se duplicaron cargas por una falla de importación. La decisión de aumentar stock se basó en un dato incorrecto. El problema no fue el cálculo del porcentaje, sino la calidad de la entrada.

7.13 Ciclo de vida de los datos

La seguridad de datos debe cubrir todo el ciclo de vida de la información. Cada etapa tiene riesgos y controles específicos.

Etapa	Riesgo principal	Control recomendado
Creación o captura	Dato incompleto o incorrecto	Controles de entrada y validaciones

Etapa	Riesgo principal	Control recomendado
Almacenamiento	Acceso indebido o pérdida	Permisos, cifrado y backup
Procesamiento	Cálculo o transformación incorrecta	Controles de proceso
Transmisión	Alteración o interceptación	Cifrado e integridad de mensajes
Consulta	Acceso no autorizado	Autorización y registros
Salida	Envío incorrecto o fuga	Controles de salida
Archivo	Conservación desordenada	Retención y clasificación
Eliminación	Recuperación indebida de datos borrados	Eliminación segura

La eliminación segura es un punto muchas veces omitido. Borrar un archivo no siempre elimina la información de manera definitiva. Discos, dispositivos móviles, impresoras, respaldos y servicios en la nube pueden conservar copias. La organización debe definir procedimientos para eliminación, especialmente al retirar equipos o finalizar contratos.

Ejemplo: una notebook entregada a un nuevo usuario sin limpieza segura puede conservar archivos del usuario anterior. Un disco retirado de un servidor puede contener bases de datos. Una impresora multifunción puede conservar documentos escaneados. Todos son riesgos de seguridad de datos.

7.14 Clasificación de datos

La clasificación de datos permite asignar niveles de protección. No todo dato requiere el mismo tratamiento. Una clasificación simple puede organizarse en cuatro niveles: público, interno, confidencial y crítico.

Clasificación	Descripción	Ejemplo	Control sugerido
Público	Puede difundirse sin daño relevante	Catálogo publicado	Control básico de integridad
Interno	Uso organizacional, no destinado al público	Manual interno	Acceso al personal correspondiente
Confidencial	Requiere acceso restringido	Legajos, contratos, datos de clientes	Permisos limitados, cifrado y registros
Crítico	Es esencial para operar o cumplir obligaciones	Base de facturación activa	Alta disponibilidad, backup, monitoreo y controles reforzados

La clasificación ayuda a decidir controles. No todo archivo necesita cifrado fuerte, doble aprobación y monitoreo especial. Pero una base con información salarial, cuentas bancarias o datos personales requiere mayores medidas. La clasificación también orienta la capacitación. El usuario debe saber cómo identificar y tratar cada tipo de dato.

La clasificación debe revisarse. Un dato puede cambiar de sensibilidad. Un reporte preliminar puede ser confidencial hasta su publicación. Una copia de respaldo de una base crítica también debe tratarse como crítica.

7.15 Respaldo, restauración y protección frente a pérdida

La disponibilidad e integridad de datos dependen en gran medida de respaldos confiables. El backup permite recuperar información ante borrado, corrupción, falla, ataque, error humano o desastre. El restore permite volver a usar esos datos.

Un plan de respaldo debe definir frecuencia, alcance, ubicación, cifrado, retención, responsables, pruebas y monitoreo. También debe proteger las copias contra modificación

o eliminación indebida. En ciertos casos conviene usar copias inmutables, que no puedan modificarse durante un período definido.

Elemento del plan de respaldo	Pregunta que debe responder
Alcance	¿Qué datos se respaldan?
Frecuencia	¿Cada cuánto se realiza la copia?
Ubicación	¿Dónde se conserva?
Retención	¿Durante cuánto tiempo se mantiene?
Cifrado	¿Cómo se protege frente a accesos indebidos?
Responsable	¿Quién administra y verifica el respaldo?
Prueba de restauración	¿Se comprobó que puede recuperarse?
Monitoreo	¿Cómo se detecta una falla del backup?

La regla 3-2-1 puede servir como referencia: tres copias de la información, dos tipos de medios o ubicaciones, una copia fuera del sitio principal o aislada. En sistemas críticos, puede agregarse una copia protegida contra cambios no autorizados.

Ejemplo: si una base de datos se actualiza cada hora y es crítica para ventas, un backup diario puede ser insuficiente. Puede requerir respaldos horarios, replicación y pruebas mensuales de restauración. La prueba es fundamental. Un respaldo que nunca fue probado puede fallar cuando más se necesita.

7.16 Seguridad de datos en integraciones y APIs

Las organizaciones intercambian datos entre sistemas internos y externos. Las integraciones pueden usar archivos, bases compartidas, colas, servicios o APIs. Cada integración introduce riesgos de confidencialidad, integridad y disponibilidad.

Riesgo en integración	Consecuencia	Control
API sin autenticación fuerte	Exposición de datos	Autenticación de sistemas y claves seguras
Archivo sin validación	Registros incorrectos	Validación de estructura y contenido
Transferencia sin cifrado	Interceptación de datos	Canal seguro
Falta de control de integridad	Archivo incompleto o alterado	Hash o firma
Error de reproceso	Duplicación o pérdida de registros	Identificadores únicos y bitácoras
Ausencia de responsable funcional	Incidentes sin dueño claro	Dueño de integración definido

Ejemplo: un sistema de ventas envía facturas al sistema contable. La integración debe validar número de comprobante, fecha, importe, impuestos, cliente y estado. Si falla el envío de cincuenta comprobantes, debe quedar registro, alerta y mecanismo de reproceso. No debe depender de una revisión manual tardía.

7.17 Datos personales y minimización

La seguridad de datos también incluye respeto por la finalidad y minimización. La minimización consiste en recolectar y conservar solo los datos necesarios para una finalidad definida. Cuantos más datos se conservan, mayor es el impacto ante una filtración y mayor el costo de protección.

En administración, muchas organizaciones solicitan datos por costumbre, no por necesidad. Esta práctica aumenta riesgos. Cada campo debería justificarse: para qué se necesita, quién lo usa, cuánto tiempo se conserva y qué control lo protege.

Práctica	Riesgo	Criterio recomendado
Recolectar datos innecesarios	Mayor impacto ante filtración	Justificar cada campo
Conservar datos indefinidamente	Aumento de exposición y costos	Definir plazos de retención
Usar datos para otra finalidad	Conflictos legales o de confianza	Respetar finalidad informada
Compartir datos sin necesidad	Pérdida de control	Limitar destinatarios
Usar datos reales para pruebas	Exposición innecesaria	Anonimizar o enmascarar

La anonimización y la seudonimización pueden reducir riesgos en análisis, reportes o pruebas. No sustituyen todos los controles, pero ayudan a limitar exposición.

7.18 Datos en ambientes de prueba

Los ambientes de prueba, desarrollo o capacitación suelen generar riesgos de seguridad. Muchas organizaciones copian datos reales de producción para probar sistemas. Si esos ambientes tienen menos controles, los datos quedan expuestos.

El uso de datos reales en prueba debe limitarse. Cuando sea posible, deben utilizarse datos sintéticos, anonimizados o enmascarados. El enmascaramiento de datos permite conservar estructura sin exponer información sensible.

Ambiente	Riesgo	Control
Desarrollo	Copias reales sin protección	Datos sintéticos o enmascarados

Ambiente	Riesgo	Control
Prueba	Permisos más amplios que producción	Controles de acceso y registros
Capacitación	Exposición de datos reales a usuarios no autorizados	Bases ficticias
Soporte externo	Acceso de proveedores a datos productivos	Contratos, permisos mínimos y monitoreo
Copias antiguas	Datos olvidados y desactualizados	Retención y eliminación programada

Ejemplo: para probar una liquidación, puede usarse una base con nombres ficticios, identificadores modificados y cuentas bancarias simuladas. Lo importante es que el proceso pueda probarse sin exponer datos reales de empleados.

Los ambientes de prueba también deben tener permisos, registros, retención y eliminación. No deben convertirse en depósitos descontrolados de copias antiguas.

7.19 Gobierno de datos

El gobierno de datos es el conjunto de roles, reglas y procesos para administrar datos. Incluye definiciones, calidad, acceso, seguridad, retención, linaje, diccionario de datos, responsables y políticas.

El gobierno de datos permite que la organización use criterios comunes. Si cada área entiende un concepto de manera diferente, los reportes no serán comparables.

Elemento del gobierno de datos	Finalidad
Dueño del dato	Asignar responsabilidad funcional
Diccionario de datos	Definir campos, formatos y significados
Linaje de datos	Conocer origen, transformación y destino

Elemento del gobierno de datos	Finalidad
Reglas de calidad	Establecer criterios de exactitud y completitud
Políticas de acceso	Definir quién puede consultar o modificar
Retención	Determinar cuánto tiempo conservar
Auditoría	Revisar uso, cambios y cumplimiento
Métricas	Medir calidad y seguridad

El linaje de datos permite saber de dónde proviene un indicador, qué transformaciones recibió y qué sistemas lo usan. Sin linaje, una diferencia entre reportes puede ser difícil de explicar.

Ejemplo: el área comercial puede considerar cliente activo a quien compró en los últimos doce meses. El área financiera puede considerarlo activo si tiene saldo pendiente. Sin definición común, un tablero puede mostrar cifras contradictorias. El gobierno de datos reduce ese problema.

7.20 Auditoría y métricas de seguridad de datos

La auditoría de seguridad de datos verifica controles, evidencias, calidad, permisos, respaldos, integridad y uso. Puede revisar accesos a bases sensibles, cambios en datos críticos, excepciones, conciliaciones, fallas de validación, resultados de restauración y reportes de calidad.

Métrica	Qué permite evaluar
Porcentaje de registros completos	Nivel de completitud
Cantidad de duplicados	Problemas de unicidad
Cantidad de accesos no justificados	Riesgo de confidencialidad
Tiempo de baja de usuarios	Rapidez para cerrar accesos

Métrica	Qué permite evaluar
Cambios críticos sin aprobación	Debilidad de integridad
Éxito de restauraciones	Capacidad real de recuperación
Errores por proceso	Calidad del procesamiento
Diferencias de conciliación	Integridad entre sistemas
Tiempo de resolución de incidentes	Eficiencia de respuesta
Antigüedad de datos críticos	Oportunidad de la información

La auditoría no debe limitarse a señalar errores. Debe verificar causas y acciones correctivas. Si todos los meses aparecen diferencias en inventario, el problema no se resuelve solo corrigiendo la planilla. Debe revisarse carga, proceso, controles físicos, capacitación y responsabilidades.

Ejemplo: una auditoría detecta que doce usuarios pueden exportar datos de nómina sin necesidad funcional. La corrección inmediata es ajustar permisos. La acción correctiva consiste en modificar el proceso de aprobación de accesos y revisar roles cada trimestre.

7.21 Matriz sintética de controles de seguridad de datos

La seguridad de datos requiere controles coordinados. La siguiente matriz resume controles relevantes según el momento del ciclo de vida.

Momento	Control principal	Finalidad
Entrada	Campos obligatorios, máscaras, validación de duplicados	Evitar datos incompletos o inválidos
Proceso	Totales de control, conciliaciones, bitácoras	Verificar tratamiento correcto

Momento	Control principal	Finalidad
Salida	Revisión de destinatarios, clasificación, cifrado	Evitar exposición o emisión incorrecta
Almacenamiento	Permisos, cifrado, backup	Proteger conservación y acceso
Transmisión	Hash, cifrado, firma digital	Proteger integridad y confidencialidad
Consulta	Autorización, logs, mínimo privilegio	Controlar acceso legítimo
Archivo	Retención, clasificación, búsqueda controlada	Conservar con orden y finalidad
Eliminación	Borrado seguro, destrucción certificada	Evitar recuperación indebida

7.22 Síntesis del capítulo

La seguridad de datos es una función central de la administración de Tecnologías de la Información. Protege la confidencialidad, integridad, disponibilidad y accesibilidad de la información que sostiene procesos organizacionales. Su valor no se limita a evitar accesos indebidos. También busca que los datos sean correctos, completos, oportunos, trazables y útiles para decidir.

Los controles de entrada, proceso y salida permiten reducir errores y detectar inconsistencias. Las validaciones impiden cargas inválidas. Las pistas de auditoría permiten reconstruir operaciones. La integridad de mensajes protege transacciones y archivos. La calidad de datos evita decisiones basadas en información deficiente. GIGO recuerda que un sistema solo puede producir buenos resultados si recibe datos adecuados.

Desde la administración, la seguridad de datos requiere roles claros, clasificación, permisos, respaldos, auditoría, métricas, gobierno de datos y mejora continua. TI implementa controles técnicos, pero las áreas de negocio deben definir reglas, significados, responsabilidades y criterios de calidad.

Para estudiantes de administración de empresas, el aprendizaje principal consiste en comprender que los datos no son un elemento secundario del sistema. Son el recurso que permite operar y decidir. Una organización que protege mal sus datos puede tener sistemas disponibles, pantallas modernas y reportes atractivos, pero decisiones incorrectas.

La seguridad de datos exige controlar quién accede, qué se carga, cómo se procesa, qué se emite, qué se conserva, qué se elimina y qué evidencia queda.

8 Seguridad de bases de datos y analítica

Las bases de datos son uno de los activos más importantes de una organización. En ellas se almacenan datos de clientes, proveedores, empleados, operaciones financieras, contratos, inventarios, pagos, facturas, configuraciones de sistemas, registros históricos y reportes utilizados para la toma de decisiones.

Desde la administración de Tecnologías de Información, una base de datos no debe verse solamente como un componente técnico. Es un recurso organizacional crítico. Si una base de datos se altera, se pierde, se expone o se consulta sin autorización, el impacto puede afectar la continuidad operativa, el cumplimiento normativo, la confianza en los reportes, la protección de datos personales, la seguridad financiera y la reputación institucional.

La seguridad de bases de datos no se limita a colocar una contraseña. Requiere definir quién puede acceder, qué datos puede ver, qué operaciones puede realizar, desde qué aplicación, bajo qué condiciones y con qué registro de auditoría. También exige proteger datos sensibles, controlar exportaciones, administrar reportes, monitorear consultas, preservar integridad y establecer responsabilidades claras sobre la calidad y el uso de la información.

La analítica agrega una complejidad adicional. Los sistemas de inteligencia de negocio, los tableros gerenciales, los reportes, los data lakes y las hojas de cálculo suelen concentrar datos provenientes de muchos sistemas. Esa concentración permite tomar mejores decisiones, pero también aumenta el riesgo de exposición, fuga, duplicación, errores de interpretación y pérdida de control.

Para estudiantes de administración de empresas, el aprendizaje central consiste en comprender que los datos tienen valor económico, legal, operativo y estratégico. Por lo tanto, deben administrarse con criterios de gobierno, seguridad, auditoría y responsabilidad.

8.1 Las bases de datos como activo organizacional

Una base de datos es un conjunto estructurado de información almacenada para ser consultada, actualizada, procesada y protegida. Puede estar vinculada con un sistema administrativo, una aplicación web, un ERP, un sistema contable, una plataforma de nómina, un CRM, una herramienta de inteligencia de negocio o un repositorio analítico.

Su valor no depende solamente de su tamaño. Una base pequeña con datos bancarios de proveedores puede ser más sensible que una base grande con información pública. La relevancia depende del tipo de datos, la función que cumplen, la criticidad para la operación y el impacto que tendría su pérdida o manipulación.

Tipo de dato	Ejemplo	Riesgo principal
Clientes	Datos de contacto, historial de compras, reclamos	Fuga de información y daño reputacional
Proveedores	Datos fiscales, cuentas bancarias, condiciones de pago	Fraude o pago indebido
Empleados	Legajos, salarios, licencias, cuentas bancarias	Exposición de datos personales

Tipo de dato	Ejemplo	Riesgo principal
Contabilidad	Asientos, saldos, comprobantes, cierres	Estados financieros incorrectos
Inventario	Stock, depósitos, movimientos	Ventas sin stock o compras innecesarias
Seguridad	Usuarios, permisos, logs, configuraciones	Acceso indebido o falta de trazabilidad
Analítica	Reportes, indicadores, modelos y tableros	Decisiones basadas en información errónea

La administración debe identificar qué bases existen, qué datos contienen, quién las usa, quién las administra, qué controles tienen y cómo se auditan.

8.2 DBMS y administración de bases de datos

Un DBMS es un sistema de gestión de bases de datos. Permite almacenar, consultar, modificar, organizar, proteger y recuperar datos. También administra usuarios, permisos, respaldos, integridad, transacciones y registros de actividad.

Desde la mirada administrativa, el DBMS cumple una función de control. No solo guarda datos. También define qué operaciones son posibles y quién puede realizarlas.

Función del DBMS	Finalidad administrativa
Gestión de usuarios	Identificar quién accede a la base
Roles y permisos	Limitar operaciones según función
Integridad referencial	Mantener relaciones consistentes entre datos
Transacciones	Evitar operaciones incompletas o inconsistentes

Función del DBMS	Finalidad administrativa
Logs	Registrar actividad para auditoría
Backups	Permitir recuperación ante pérdida
Cifrado	Proteger datos ante acceso no autorizado
Vistas y procedimientos	Controlar consultas y operaciones permitidas

Ejemplo: un sistema de facturación puede usar una base de datos para guardar clientes, comprobantes, impuestos y pagos. Si el DBMS permite que cualquier usuario modifique registros directamente, los controles de la aplicación pueden quedar anulados. Por eso, el acceso directo a la base debe restringirse y auditarse.

8.3 Usuarios, roles y permisos

El control de acceso a una base de datos determina quién puede conectarse, qué operaciones puede realizar y sobre qué datos. Es uno de los controles más importantes porque una mala configuración puede exponer información o permitir modificaciones indebidas.

Los usuarios pueden ser personas, aplicaciones o procesos automáticos. No todos deberían tener el mismo nivel de acceso. Una aplicación de reportes puede necesitar leer datos, pero no modificarlos. Un analista puede necesitar consultar ventas agregadas, pero no acceder a datos de nómina. Un administrador de base puede necesitar realizar tareas técnicas, pero su actividad debe registrarse.

Tipo de usuario	Necesidad típica	Riesgo si tiene permisos excesivos
Usuario operativo	Consultar o cargar datos de su área	Acceso a información que no corresponde

Tipo de usuario	Necesidad típica	Riesgo si tiene permisos excesivos
Analista	Leer información para reportes	Exportaciones masivas o exposición de datos sensibles
Aplicación	Ejecutar operaciones específicas	Daño amplio si la cuenta es comprometida
Administrador de base	Mantener estructura, rendimiento y seguridad	Modificación directa sin control
Proveedor externo	Soporte o mantenimiento	Acceso de tercero sin monitoreo
Cuenta de servicio	Integraciones o procesos automáticos	Permisos elevados olvidados

El uso de roles permite agrupar permisos. En lugar de configurar cada usuario individualmente, se definen perfiles como “solo lectura”, “analista comercial”, “operador de pagos”, “administrador técnico” o “consulta gerencial”. Esto facilita la administración y reduce errores.

8.4 Principio de mínimo privilegio

El principio de mínimo privilegio establece que cada usuario, aplicación o proceso debe tener únicamente los permisos necesarios para cumplir su función. No debe otorgarse acceso por comodidad, costumbre o prevención genérica.

En bases de datos, este principio es especialmente importante porque un permiso excesivo puede permitir copiar, modificar, borrar o exponer grandes volúmenes de información.

Situación	Problema	Corrección
Aplicación con permiso de administrador	Riesgo de daño total ante compromiso	Limitar a operaciones necesarias
Analista con acceso a todas las tablas	Exposición de datos sensibles	Acceso mediante vistas o reportes filtrados
Usuario de soporte con acceso permanente	Riesgo de tercero	Acceso temporal y monitoreado
Cuenta de servicio sin responsable	Falta de control	Asignar dueño y revisar permisos
Usuario con permisos heredados	Acumulación de privilegios	Recertificación periódica

Ejemplo: una auditoría identifica que la cuenta de la aplicación de facturación tiene permisos de administrador completo sobre la base. La aplicación solo necesita insertar facturas y consultar clientes activos. El exceso de permisos se originó durante el desarrollo y nunca se corrigió. La solución consiste en redefinir permisos según la operación real que debe ejecutar.

8.5 Vistas como mecanismo de control

Una vista es una consulta predefinida que muestra un subconjunto de datos de una o varias tablas. Permite que un usuario acceda solo a las columnas y filas necesarias, sin acceder directamente a la tabla completa.

Las vistas son útiles cuando distintas áreas necesitan consultar información de una misma base, pero con diferentes niveles de detalle.

Usuario o área	Dato necesario	Dato que debería ocultarse
Atención al cliente	Nombre, número de cliente, estado de reclamo	Datos bancarios o salariales

Usuario o área	Dato necesario	Dato que debería ocultarse
Comercial	Historial de compras y saldo comercial	Documento completo o datos sensibles
Dirección	Indicadores agregados	Datos personales individuales
Auditoría	Datos requeridos para revisión	Información no vinculada con el alcance
Soporte técnico	Identificador de error o transacción	Contenido sensible del cliente

Ejemplo: el área comercial necesita conocer historial de compras y saldo pendiente. Se crea una vista que muestra código de cliente, zona, compras y saldo, pero no muestra documento, dirección particular ni información bancaria.

La ventaja administrativa es clara: se permite trabajar con datos útiles sin exponer toda la información disponible.

8.6 Stored procedures como control de operación

Un stored procedure es un procedimiento almacenado en la base de datos. Contiene instrucciones que ejecutan una operación específica. Permite controlar qué puede hacer el usuario sin permitir acceso directo a las tablas.

En lugar de permitir que un usuario escriba consultas libres, se le permite ejecutar una operación definida. Esto reduce el riesgo de errores, accesos indebidos o manipulación directa.

Uso de stored procedure	Beneficio
Consultar saldo de cliente	Devuelve solo datos autorizados
Registrar una operación	Aplica validaciones internas

Uso de stored procedure	Beneficio
Actualizar estado de una transacción	Controla reglas de negocio
Generar reporte limitado	Evita consulta directa a tablas sensibles
Procesar datos masivos	Estandariza el procedimiento

Ejemplo: atención al cliente necesita consultar saldo por DNI. En lugar de dar acceso directo a la tabla de cuentas, se crea un procedimiento que recibe el DNI, valida el perfil del usuario y devuelve solo nombre y saldo. El operador no puede listar todos los clientes ni modificar registros.

Los procedimientos almacenados también ayudan a reducir riesgos de inyección SQL, siempre que estén correctamente diseñados y usen parámetros seguros.

8.7 Auditoría de consultas

La auditoría de consultas registra operaciones realizadas sobre la base de datos. Permite saber quién accedió, qué consultó, cuándo, desde dónde, qué cantidad de registros obtuvo y qué cambios realizó.

Este registro es esencial para investigar incidentes, detectar conductas anómalas, cumplir obligaciones legales y sostener auditorías internas.

Evento a registrar	Utilidad
Autenticaciones exitosas	Identificar accesos válidos
Intentos fallidos	Detectar ataques o errores
Consultas sobre datos sensibles	Controlar acceso a información crítica
Inserciones	Conocer quién creó registros
Modificaciones	Reconstruir cambios
Eliminaciones	Investigar pérdida de datos

Evento a registrar	Utilidad
Cambios de estructura	Controlar alteraciones técnicas
Accesos administrativos	Supervisar cuentas privilegiadas
Exportaciones	Detectar posibles fugas

Ejemplo: si un usuario consulta 180.000 registros de clientes en quince minutos, el registro de auditoría permite identificar usuario, hora, origen y tipo de consulta. Sin ese registro, la organización puede detectar la fuga, pero no reconstruirla con precisión.

8.8 Monitoreo de actividad de bases de datos

El monitoreo de actividad de bases de datos analiza los registros para detectar patrones anómalos. No alcanza con registrar lo que ocurre. También debe revisarse cuando algo se aparta de lo normal.

Las herramientas de DAM permiten automatizar esa tarea. Generan alertas cuando una consulta, acceso o modificación supera parámetros esperados.

Comportamiento anómalo	Riesgo posible
Consulta masiva fuera del horario habitual	Extracción no autorizada
Acceso a tabla sensible desde IP inusual	Cuenta comprometida
Muchos intentos fallidos	Ataque o credenciales incorrectas
Cambio estructural no aprobado	Alteración del sistema
Exportación de base completa	Fuga de información
Acceso de administrador sin ticket	Actividad privilegiada no justificada
Consultas frecuentes a nómina por usuario no autorizado	Abuso de privilegios

Ejemplo: un sistema de monitoreo detecta que un usuario de marketing consultó volúmenes de datos cuarenta veces superiores a su actividad habitual. La alerta permite investigar antes de que la información sea usada fuera de la organización.

8.9 Protección de datos sensibles

No todos los datos requieren el mismo nivel de protección. Los datos personales, financieros, laborales, estratégicos o confidenciales deben tratarse con controles más estrictos.

La clasificación de datos permite decidir qué medidas aplicar.

Clasificación	Ejemplo	Control sugerido
Público	Información publicada en sitio web	Control básico de integridad
Interno	Manuales, comunicaciones internas	Acceso a personal autorizado
Confidencial	Contratos, clientes, precios, reportes	Restricción de acceso y registros
Sensible	Salud, biometría, datos salariales	Cifrado, mínimo privilegio y monitoreo
Crítico	Base de facturación o pagos	Alta disponibilidad, backup y auditoría

La protección debe aplicarse en producción, desarrollo, prueba, reportes, exportaciones, backups y data lakes. Un dato sensible no deja de ser sensible por estar en una copia de prueba o en una hoja de cálculo.

8.10 Enmascaramiento de datos

El enmascaramiento de datos sustituye datos reales por valores ficticios o parcialmente ocultos, manteniendo formato y utilidad operativa. Se utiliza cuando el usuario o el proceso no necesita ver el dato real completo.

Puede ser estático o dinámico. El enmascaramiento estático genera una copia de datos modificados, normalmente para desarrollo o prueba. El enmascaramiento dinámico muestra datos ocultos en tiempo real según el perfil del usuario, sin modificar el dato original.

Tipo de enmascaramiento	Característica	Ejemplo
Estático	Crea una copia con datos reemplazados	Base de prueba con nombres ficticios
Dinámico	Oculta datos al consultar según usuario	Ver solo últimos 4 dígitos de una cuenta
Parcial	Muestra una parte del dato	Documento XXX.XXX.123
Total	Reemplaza completamente el dato	Nombre convertido en valor ficticio

Ejemplo: un analista de soporte necesita ver que existe una cuenta bancaria cargada, pero no necesita conocerla completa. El sistema muestra solo los últimos cuatro dígitos. De esta forma se conserva utilidad operativa y se reduce exposición.

8.11 Anonimización y seudonimización

La anonimización transforma los datos de forma tal que ya no sea posible identificar a la persona. Si la anonimización es efectiva e irreversible, los datos dejan de ser personales en muchos marcos normativos.

La seudonimización reemplaza identificadores directos por códigos, pero conserva la posibilidad de reidentificar mediante una tabla de correspondencia guardada por separado. Por eso, los datos seudonimizados siguen siendo datos personales.

Técnica	¿Permite reidentificar?	Uso típico
Anonimización	No, si está bien aplicada	Estadísticas, investigación, análisis agregado
Seudonimización	Sí, mediante tabla separada	Análisis con posibilidad de seguimiento controlado
Enmascaramiento	Depende del método	Desarrollo, pruebas, soporte, reportes limitados

Ejemplo: una organización analiza reclamos de clientes. Si elimina identificadores y conserva solo datos agregados por región y tipo de reclamo, puede usar anonimización. Si reemplaza el cliente por un código y conserva una tabla para volver a identificarlo, se trata de seudonimización.

La selección de técnica depende de la finalidad. Si no es necesario volver a identificar, la anonimización reduce el riesgo en mayor medida.

8.12 DLP: prevención de fuga de datos

DLP significa prevención de pérdida de datos. Es el conjunto de controles que detectan, alertan o bloquean salidas no autorizadas de información sensible.

Puede operar en correo electrónico, dispositivos, red, almacenamiento en la nube, aplicaciones, herramientas de reportes o puntos de exportación.

Punto de control DLP	Ejemplo de riesgo controlado
Correo electrónico	Envío de base con datos personales a destinatario externo

Punto de control DLP	Ejemplo de riesgo controlado
Dispositivo del usuario	Copia de archivos sensibles a pendrive
Red	Transferencia masiva a destino no autorizado
Nube	Subida a repositorio personal
Aplicación	Exportación masiva desde sistema interno
BI	Descarga de reportes sensibles
Endpoint	Archivo con datos críticos guardado localmente

Ejemplo: una regla de DLP bloquea correos salientes con adjuntos que contienen más de cien números de documento. Algunos casos pueden ser legítimos, pero deben redirigirse a canales aprobados y con autorización. Otros pueden indicar intento de fuga.

El DLP requiere clasificación de datos. Si la organización no sabe qué datos son sensibles, la herramienta no puede decidir correctamente qué bloquear o alertar.

8.13 Integridad referencial

La integridad referencial asegura que las relaciones entre tablas sean coherentes. Si una factura está asociada a un cliente, ese cliente debe existir. Si una orden de compra refiere a un proveedor, ese proveedor debe existir.

En bases de datos relacionales, esta integridad se controla mediante claves primarias y claves foráneas. Su ausencia puede generar registros huérfanos, inconsistencias y errores en reportes.

Relación	Problema si falla la integridad
Factura-cliente	Facturas sin cliente válido

Relación	Problema si falla la integridad
Pago-proveedor	Pagos sin proveedor existente
Orden de compra-producto	Compras de productos inexistentes
Empleado-liquidación	Liquidaciones sin empleado activo
Asiento-cuenta contable	Registros en cuentas inexistentes
Inventario-depósito	Stock asignado a depósito inválido

Ejemplo: si el sistema permite facturas sin cliente válido, los reportes de ventas pueden mostrar importes que no pueden atribuirse correctamente. Esto afecta análisis comercial, contabilidad y auditoría.

La integridad referencial no es solo un tema técnico. Es una condición para la confiabilidad administrativa de la información.

8.14 Datos maestros

Los datos maestros son registros de referencia que se usan en múltiples procesos. Incluyen clientes, proveedores, empleados, productos, cuentas contables, centros de costo, condiciones de pago, listas de precios y cuentas bancarias.

Un error en datos maestros se propaga. Si una cuenta bancaria de proveedor está mal cargada, los pagos pueden desviarse. Si una cuenta contable está mal parametrizada, los asientos pueden registrarse incorrectamente durante meses.

Dato maestro	Campo crítico	Riesgo
Proveedor	CBU o cuenta bancaria	Pago a cuenta equivocada
Cliente	Condición fiscal	Facturación incorrecta
Producto	Precio o unidad de medida	Venta o stock incorrecto
Empleado	Cuenta bancaria o categoría	Liquidación o pago erróneo

Dato maestro	Campo crítico	Riesgo
Cuenta contable	Clasificación	Estados financieros distorsionados
Centro de costo	Asignación	Presupuesto o reporte incorrecto

Los cambios en datos maestros deben controlarse. Debe existir solicitud, aprobación, registro de usuario, fecha, valor anterior, valor nuevo y documentación respaldatoria cuando corresponda.

8.15 Controles sobre cambios en datos maestros

Los datos maestros requieren controles reforzados porque afectan muchas transacciones. La modificación de un dato maestro puede ser más riesgosa que una operación individual.

Control	Finalidad
Solicitud formal	Justificar el cambio
Aprobación independiente	Evitar modificaciones unilaterales
Registro de valor anterior y nuevo	Permitir reconstrucción
Documentación respaldatoria	Validar legitimidad
Alerta por campos críticos	Detectar cambios sensibles
Bloqueo temporal de pagos	Reducir riesgo de fraude
Revisión periódica	Identificar cambios inusuales
Segregación de funciones	Evitar concentración de tareas

Ejemplo: se revisan cambios de CBU de proveedores. Se detecta que algunos fueron realizados fuera del horario habitual y sin aprobación. Si luego hubo pagos a esos proveedores, el riesgo de fraude es alto. La auditoría debe revisar logs, documentación, aprobadores, fechas y cuentas destino.

8.16 Seguridad en reportes y BI

Los sistemas de BI y reportes permiten consolidar información para la toma de decisiones. Su valor es alto, pero también su riesgo. Un reporte puede contener información financiera, comercial, salarial, de clientes o estratégica.

El hecho de que los datos aparezcan en un tablero visual no reduce su sensibilidad. Si un reporte muestra nómina por persona, márgenes por producto, clientes con montos de compra o datos de proveedores, debe tener controles de acceso.

Riesgo en BI	Control recomendado
Todos los usuarios ven todos los reportes	RBAC y segmentación por perfil
Reportes con datos sensibles	Clasificación y permisos específicos
Descargas sin registro	Log de exportaciones
Distribución por correo	Canales aprobados y destinatarios controlados
Datos desactualizados	Fecha de actualización visible
Indicadores mal definidos	Diccionario y gobierno de datos
Falta de trazabilidad	Linaje de datos documentado

Ejemplo: una plataforma de BI contiene reportes sin restricciones. Algunos muestran nómina, márgenes comerciales y datos individuales de clientes. La organización debe clasificar reportes, asignar responsables, definir permisos y auditar accesos.

8.17 Control de acceso basado en roles en BI

RBAC significa control de acceso basado en roles. Permite asignar permisos según el rol del usuario y no según decisiones aisladas.

En BI, RBAC es fundamental porque un mismo tablero puede mostrar diferentes niveles de información según el perfil. Un director puede ver información agregada. Un

responsable de área puede ver su sector. Un analista puede ver datos operativos, pero no información salarial o confidencial.

Rol	Acceso razonable
Dirección general	Indicadores agregados y estratégicos
Gerencia de ventas	Ventas, clientes y márgenes de su área
Recursos Humanos	Nómina y datos laborales autorizados
Finanzas	Costos, pagos, cobranzas y saldos
Analista comercial	Datos necesarios para análisis, preferentemente agregados
Auditoría	Acceso según alcance aprobado
Usuario operativo	Reportes limitados a su proceso

El acceso a reportes debe revisarse periódicamente. Un usuario que cambió de área puede conservar acceso a reportes que ya no corresponden a su función.

8.18 Riesgos de exportación a hojas de cálculo

La exportación a hojas de cálculo es una práctica común. También es uno de los principales riesgos de fuga de información. Cuando los datos salen del sistema o de la plataforma de BI, pierden muchos controles originales.

Un archivo exportado puede guardarse localmente, enviarse por correo, copiarse a un pendrive, subirse a una nube personal o quedar olvidado en una computadora.

Riesgo de exportación	Ejemplo	Control
Archivo local sin protección	Planilla con salarios en escritorio	Cifrado y eliminación segura

Riesgo de exportación	Ejemplo	Control
Envío por correo	Base de clientes enviada externamente	DLP y canales autorizados
Copia a USB	Reporte sensible en pendrive	Bloqueo o control de dispositivos
Reenvío informal	PDF compartido sin autorización	Marca de agua y permisos
Falta de trazabilidad	No se sabe quién descargó	Log de exportaciones
Datos desactualizados	Decisiones sobre copia vieja	Fecha de extracción visible

Ejemplo: un analista exporta salarios de empleados para un análisis y guarda el archivo localmente. Luego el equipo es reasignado sin limpieza adecuada. La información queda expuesta. El problema no está en la base original, sino en la copia exportada.

8.19 Data lakes

Un data lake es un repositorio que almacena grandes volúmenes de datos en formato original o poco transformado. Puede recibir datos de sistemas transaccionales, logs, sensores, archivos, imágenes, plataformas externas y fuentes analíticas.

Su ventaja es la flexibilidad. Su riesgo también. Al concentrar datos variados, puede acumular información sensible sin clasificación clara.

Riesgo en data lake	Consecuencia
Datos sin clasificación	Accesos inadecuados
Acceso amplio a analistas	Exposición innecesaria
Datos personales mezclados con operativos	Dificultad de cumplimiento

Riesgo en data lake	Consecuencia
Falta de catálogo	No se sabe qué datos existen
Duplicación de fuentes	Reportes contradictorios
Retención indefinida	Mayor exposición
Dificultad para supresión	Problemas ante derechos de titulares
Falta de linaje	No se conoce origen ni transformación

Ejemplo: un data lake recibe datos de ventas, clientes, reclamos, navegación web y logs. Si no se clasifica cada conjunto de datos, un analista puede acceder a datos personales que no necesita. Además, puede ser difícil responder solicitudes de supresión o rectificación.

8.20 Gobierno de datos

El gobierno de datos es el conjunto de políticas, roles, responsabilidades, definiciones y controles que permiten administrar los datos como activos organizacionales.

No es una función exclusivamente técnica. Requiere participación de las áreas de negocio, TI, auditoría, seguridad, legal y dirección.

Elemento del gobierno de datos	Finalidad
Catálogo de datos	Saber qué datos existen y dónde están
Propietario del dato	Asignar autoridad funcional
Administrador del dato	Gestionar calidad y definición
Custodio del dato	Implementar controles técnicos
Clasificación	Definir sensibilidad y controles
Diccionario de datos	Acordar significado de campos

Elemento del gobierno de datos	Finalidad
Linaje de datos	Conocer origen, transformación y destino
Calidad de datos	Detectar errores, duplicados e inconsistencias
Retención	Definir conservación y eliminación
Auditoría	Verificar uso, acceso y cumplimiento

Sin gobierno de datos, cada área puede definir los mismos conceptos de manera distinta. Esto genera reportes contradictorios y decisiones inconsistentes.

8.21 Roles del gobierno de datos

Tres roles son especialmente relevantes: data owner, data steward y data custodian.

Rol	Traducción funcional	Responsabilidad
Data owner	Propietario del dato	Define uso, acceso, calidad esperada y reglas funcionales
Data steward	Administrador del dato	Mantiene definiciones, calidad y consistencia
Data custodian	Custodio del dato	Implementa controles técnicos, respaldo y seguridad

Ejemplo: el director financiero puede ser propietario de los datos contables. Un analista contable puede actuar como administrador del dato, cuidando definiciones y calidad. TI actúa como custodio técnico, configurando permisos, backups y seguridad.

Este esquema evita una confusión frecuente: TI no debe decidir por sí sola quién puede ver datos de nómina o proveedores. Esa decisión corresponde al dueño funcional del dato, con implementación técnica por parte de TI.

8.22 Catálogo de datos y diccionario de datos

El catálogo de datos es un inventario organizado de los conjuntos de datos de la organización. Indica dónde están, quién es responsable, qué contienen, qué sensibilidad tienen, de dónde provienen y cómo se usan.

El diccionario de datos define el significado de campos, indicadores y conceptos. Evita que distintas áreas usen la misma palabra con significados diferentes.

Herramienta	Qué responde
Catálogo de datos	¿Qué datos existen, dónde están y quién es responsable?
Diccionario de datos	¿Qué significa cada dato o indicador?
Linaje de datos	¿De dónde viene el dato y cómo se transforma?
Clasificación	¿Qué nivel de sensibilidad tiene?
Reglas de calidad	¿Qué condiciones debe cumplir?

Ejemplo: doce sistemas tienen una tabla llamada “clientes”. En algunos casos incluye clientes activos, en otros prospectos y en otros personas físicas y jurídicas mezcladas. Sin diccionario, cada área reporta cifras distintas. Con gobierno de datos, se acuerdan definiciones y se reducen inconsistencias.

8.23 Linaje de datos

El linaje de datos permite conocer el recorrido de un dato desde su origen hasta su uso final. Indica de qué sistema proviene, qué transformaciones recibió, en qué reportes aparece y qué decisiones alimenta.

En analítica, el linaje es fundamental porque los datos suelen pasar por muchas etapas antes de llegar a un tablero.

Etapa	Pregunta de linaje
Origen	¿De qué sistema proviene el dato?
Extracción	¿Cuándo y cómo se obtuvo?
Transformación	¿Qué reglas se aplicaron?
Carga	¿Dónde se almacenó?
Reporte	¿En qué tablero o informe aparece?
Uso	¿Qué decisión apoya?
Responsable	¿Quién valida su definición?

Ejemplo: un indicador de "ventas netas" puede excluir impuestos, anulaciones y devoluciones en un área, pero no en otra. Sin linaje y definición común, el reporte puede parecer exacto y al mismo tiempo ser conceptualmente incorrecto.

8.24 Seguridad, auditoría y cumplimiento

La seguridad de bases de datos se relaciona directamente con auditoría y cumplimiento. Los logs permiten verificar accesos. Los controles sobre datos maestros permiten detectar modificaciones indebidas. El cifrado protege información sensible. El gobierno de datos ayuda a cumplir obligaciones de protección de datos personales.

Necesidad de auditoría o cumplimiento	Control de base de datos
Verificar quién accedió a datos sensibles	Auditoría de consultas
Probar integridad de cambios	Log con valor anterior y nuevo
Proteger datos personales	Cifrado, permisos y minimización
Investigar fraude	DAM, logs y pistas de auditoría

Necesidad de auditoría o cumplimiento	Control de base de datos
Cumplir Ley 25.326	Seguridad, acceso limitado y derechos del titular
Controlar datos maestros	Aprobación y revisión de cambios
Garantizar recuperación	Backups y pruebas de restauración

Ejemplo: una auditoría interna revisa cambios de cuentas bancarias de proveedores. Necesita logs completos, valor anterior, valor nuevo, usuario, fecha, aprobación y documentación respaldatoria. Si esos registros no existen, la investigación queda debilitada.

8.25 Matriz integradora de riesgos y controles

La siguiente matriz resume los principales riesgos de seguridad en bases de datos y analítica.

Riesgo	Impacto posible	Control recomendado
Permisos excesivos	Acceso o modificación indebida	Mínimo privilegio y roles
Acceso directo a tablas sensibles	Exposición de datos	Vistas y stored procedures
Falta de logs	Imposibilidad de investigar	Auditoría de consultas
Consultas masivas no detectadas	Fuga de información	DAM y alertas
Datos sensibles visibles	Exposición innecesaria	Enmascaramiento, anonimización o seudonimización

Riesgo	Impacto posible	Control recomendado
Exportaciones a hojas de cálculo	Pérdida de control	DLP y registro de descargas
Cambios en datos maestros sin aprobación	Fraude o error operativo	Flujo de aprobación y log completo
Ausencia de integridad referencial	Registros inconsistentes	Claves foráneas y controles de base
BI sin control por roles	Acceso indebido a reportes	RBAC y clasificación
Data lake sin gobierno	Acumulación descontrolada de datos	Catálogo, clasificación y linaje
Sin responsable del dato	Decisiones difusas	Data owner y data steward
Backups no protegidos	Fuga o pérdida de datos	Cifrado y prueba de restauración

8.26 Síntesis del capítulo

La seguridad de bases de datos y analítica es una función crítica dentro de la administración de Tecnologías de Información. Las bases de datos concentran activos de información que sostienen operaciones, reportes, decisiones, cumplimiento legal y continuidad del negocio. Por esa razón, deben protegerse con controles técnicos y administrativos.

El control de acceso debe basarse en usuarios, roles, permisos y mínimo privilegio. Las vistas y los stored procedures permiten limitar la exposición directa de tablas sensibles. La auditoría de consultas y el monitoreo de actividad permiten detectar accesos inusuales, consultas masivas y cambios no autorizados. Las técnicas de enmascaramiento, anonimización y seudonimización reducen la exposición de datos sensibles cuando el acceso completo no es necesario.

La dimensión analítica exige cuidados adicionales. Los reportes de BI, las exportaciones a hojas de cálculo y los data lakes pueden dispersar información fuera del entorno transaccional original. Si esos datos no se clasifican, no se controlan y no tienen responsables definidos, la organización pierde visibilidad sobre uno de sus activos más importantes.

El gobierno de datos proporciona el marco necesario para administrar esa complejidad. Define propietarios, administradores, custodios, catálogos, diccionarios, linaje, calidad, retención y controles. Sin gobierno de datos, los controles técnicos operan sin dirección y los reportes pueden volverse inconsistentes.

Para estudiantes de administración de empresas, el aprendizaje central consiste en comprender que los datos no pertenecen únicamente al área técnica. Son activos organizacionales. Deben tener propietario, finalidad, reglas de acceso, controles de uso, calidad verificable y mecanismos de auditoría.

9 Seguridad de los dispositivos finales (endpoints)

La seguridad en dispositivos finales se ocupa de proteger los equipos desde los cuales las personas acceden a los sistemas, documentos, aplicaciones, redes y servicios de una organización. En esta categoría se incluyen notebooks, computadoras de escritorio, teléfonos celulares, tabletas, terminales de atención, equipos de punto de venta y otros dispositivos utilizados para trabajar con información institucional.

Estos equipos son relevantes porque constituyen el punto de contacto entre el usuario y la organización digital. Desde ellos se consulta el correo, se cargan operaciones, se aprueban pagos, se descargan reportes, se accede a plataformas en la nube, se participa en reuniones, se almacenan documentos y se gestionan tareas administrativas. Por esa razón, un dispositivo final mal protegido puede convertirse en una puerta de entrada a datos sensibles, sistemas críticos o procesos de negocio.

Desde la administración de Tecnologías de Información, el problema no debe entenderse solo como una cuestión técnica. Una notebook robada, un celular perdido, un usuario con permisos excesivos, un pendrive infectado, una aplicación no autorizada o una

computadora sin actualizaciones pueden generar impactos operativos, económicos, legales y reputacionales. El riesgo no está únicamente en el equipo físico, sino en la información, las credenciales y los accesos que ese equipo permite utilizar.

La seguridad de dispositivos finales requiere políticas, inventario, configuración segura, cifrado, actualizaciones, protección contra software malicioso, control de aplicaciones, gestión de privilegios, administración de dispositivos móviles, reglas para trabajo remoto, controles sobre dispositivos personales y procedimientos de respuesta ante incidentes. Cada dispositivo debe ser tratado como un activo de información sometido a control, seguimiento y auditoría.

9.1 Concepto de dispositivo final

Un dispositivo final es todo equipo que permite a una persona interactuar con sistemas, aplicaciones, redes o información de una organización. Se lo denomina también *endpoint*, porque se ubica en el extremo de la red desde donde el usuario trabaja.

En una organización, los dispositivos finales no son elementos secundarios. En muchos casos concentran más riesgo que los servidores centrales, porque se encuentran distribuidos, se conectan desde distintos lugares, son utilizados por personas con diferentes niveles de capacitación y pueden contener copias locales de información sensible.

Tipo de dispositivo	Uso frecuente	Riesgo principal
Notebook	Trabajo administrativo, remoto o móvil	Pérdida, robo, exposición de datos y sesiones abiertas
Computadora de escritorio	Trabajo en oficina o puesto fijo	Software no autorizado, privilegios excesivos y falta de actualización

Tipo de dispositivo	Uso frecuente	Riesgo principal
Celular	Correo, mensajería, autenticación y aplicaciones corporativas	Pérdida, acceso no autorizado y mezcla de datos personales y laborales
Tableta	Trabajo móvil, atención al público o relevamiento	Robo, sincronización no controlada y falta de gestión centralizada
Terminal de punto de venta	Operaciones comerciales y cobros	Fraude, manipulación de software y exposición de transacciones
Equipo compartido	Aulas, recepción, laboratorios o atención	Uso por múltiples personas y baja trazabilidad

La administración debe conocer qué dispositivos existen, quién los usa, qué datos almacenan, qué sistemas permiten acceder, qué controles tienen y qué ocurre cuando se pierden, se dañan, se reasignan o dejan de usarse.

9.2 Por qué los dispositivos finales son críticos para la organización

Los dispositivos finales son críticos porque combinan tres elementos: acceso, datos y usuario. Un equipo puede tener credenciales guardadas, sesiones activas, archivos descargados, certificados, aplicaciones instaladas y permisos sobre sistemas institucionales. Si ese equipo queda fuera de control, el riesgo alcanza a toda la organización.

Un error frecuente consiste en considerar que el endpoint es responsabilidad individual del usuario. Ese enfoque es insuficiente. El usuario debe cuidar el dispositivo, pero la organización debe establecer controles. La seguridad no puede depender solo de la buena voluntad o del conocimiento personal de cada empleado.

Elemento comprometido	Consecuencia posible
Equipo físico	Pérdida económica y posible exposición de datos
Datos locales	Filtración, copia no autorizada o pérdida de información
Credenciales	Acceso indebido a sistemas institucionales
Sesiones abiertas	Uso del sistema sin conocer contraseña
Software instalado	Ingreso de malware o herramientas no permitidas
Configuración	Debilitamiento de controles de seguridad
Conectividad	Propagación de incidentes hacia la red corporativa

El riesgo debe evaluarse según el contexto. No tiene la misma criticidad una computadora de uso general sin datos sensibles que una notebook del área financiera con acceso a sistemas de pagos, datos bancarios de proveedores y correo institucional.

9.3 Notebooks: movilidad y exposición

Las notebooks presentan un riesgo particular porque son portátiles. Pueden trasladarse entre la oficina, el hogar, aulas, reuniones, viajes, espacios compartidos y redes públicas. Esa movilidad aumenta la probabilidad de pérdida, robo, daño físico y conexión a entornos inseguros.

Una notebook de trabajo suele contener documentos, planillas, correos, accesos a plataformas, aplicaciones internas y archivos temporales. Aunque la organización utilice sistemas en la nube, es frecuente que los usuarios descarguen reportes o guarden copias locales.

Control	Finalidad administrativa
Cifrado de disco	Reducir la exposición de datos ante pérdida o robo
Bloqueo de pantalla	Evitar uso indebido cuando el usuario se ausenta
Protección contra malware	Detectar y bloquear software malicioso
Actualizaciones periódicas	Corregir vulnerabilidades conocidas
Inventario	Saber qué equipo existe y a quién está asignado
Respaldo de información	Evitar pérdida de datos locales relevantes
Borrado remoto	Eliminar información institucional si el equipo se pierde
Restricción de privilegios	Evitar instalaciones o cambios no autorizados

Ejemplo: una notebook utilizada por un analista de administración contiene archivos de clientes y proveedores. El equipo es robado durante un traslado. Si el disco está cifrado, el usuario tiene bloqueo de pantalla y la organización puede revocar sesiones, el incidente tendrá un impacto controlado. Si no existen esos controles, la organización debe considerar que los datos pudieron quedar expuestos.

9.4 Celulares y tabletas: el riesgo de la movilidad permanente

Los celulares y tabletas tienen una particularidad: acompañan al usuario de manera permanente. Se usan para correo, mensajería, autenticación, documentos, aplicaciones corporativas, videollamadas y acceso a plataformas. También suelen combinar uso personal y laboral.

El celular puede ser más sensible que una computadora, porque muchas veces contiene códigos de autenticación, cuentas abiertas, historial de mensajes, archivos descargados y aplicaciones de acceso corporativo. Además, su pérdida puede detectarse tarde o minimizarse por tratarse de un dispositivo de uso cotidiano.

Riesgo en celulares	Ejemplo
Pérdida o robo	El dispositivo queda en un transporte o lugar público
Falta de bloqueo	Cualquier persona puede acceder a correo o mensajería
Aplicaciones no autorizadas	Una aplicación accede a contactos, archivos o ubicación
Capturas de pantalla	Se guardan imágenes de información sensible
Uso de cuentas personales	Documentos institucionales se sincronizan fuera del control corporativo
Sesiones abiertas	Un tercero puede ingresar sin conocer la contraseña
Falta de actualización	El sistema conserva vulnerabilidades conocidas

El control de celulares y tabletas debe contemplar bloqueo de pantalla, cifrado, actualización, capacidad de borrado remoto, separación entre datos personales y laborales, administración centralizada y procedimientos ante pérdida.

9.5 Inventario de dispositivos finales

El inventario es la base de la seguridad. No se puede proteger lo que no se conoce. Un inventario de dispositivos finales debe permitir saber qué equipos existen, dónde están, a

quién pertenecen, quién los utiliza, qué sistema operativo tienen, qué controles están activos y cuál es su estado de cumplimiento.

Campo del inventario	Utilidad
Identificador del equipo	Evita confusiones entre dispositivos similares
Tipo de dispositivo	Permite diferenciar notebook, celular, tableta o PC
Usuario asignado	Determina responsabilidad operativa
Área o sector	Relaciona el equipo con procesos de negocio
Sistema operativo	Permite controlar versiones y soporte
Estado de cifrado	Indica si los datos locales están protegidos
Estado de protección antimalware	Permite verificar cobertura
Última conexión	Identifica equipos fuera de visibilidad
Estado de actualizaciones	Muestra deuda de parches
Fecha de alta, reasignación o baja	Aporta trazabilidad del ciclo de vida

Ejemplo: una organización declara tener 180 notebooks, pero el sistema de gestión solo recibe reportes de 145. Las 35 restantes pueden estar apagadas, fuera de uso, perdidas, mal configuradas o utilizadas sin controles. Esa diferencia no es menor: representa una zona ciega para la seguridad y la auditoría.

9.6 Cifrado de disco

El cifrado de disco protege la información almacenada en el dispositivo. Si una persona obtiene físicamente el equipo, no debería poder leer los archivos sin las credenciales o

claves correspondientes. Es un control básico para notebooks, celulares y equipos que almacenan información sensible.

El cifrado no evita el robo del dispositivo, pero reduce el impacto del incidente. Desde administración, esto permite distinguir entre pérdida del activo físico y exposición de datos. La pérdida de una notebook cifrada no tiene la misma gravedad que la pérdida de una notebook sin cifrado que contiene información de clientes, nómina o proveedores.

Situación	Sin cifrado	Con cifrado
Robo de notebook	El disco puede leerse desde otro equipo	Los datos permanecen protegidos sin clave
Equipo enviado a reparación	El proveedor podría acceder a archivos	El acceso queda limitado
Reasignación sin borrado adecuado	El nuevo usuario puede ver datos anteriores	El riesgo se reduce si se combina con borrado seguro
Pérdida de celular	Pueden quedar expuestos correos o archivos	El acceso requiere autenticación y claves

El cifrado debe gestionarse con políticas y evidencia. La organización debe poder demostrar qué porcentaje de equipos está cifrado, cómo se custodian claves de recuperación y qué excepciones existen.

9.7 Bloqueo de pantalla y control de sesión

El bloqueo de pantalla es un control simple, pero relevante. Evita que una persona utilice un equipo cuando el usuario legítimo se ausenta. Debe aplicarse a computadoras, notebooks, celulares y tabletas.

La política debe definir el tiempo máximo de inactividad. En equipos que manejan información sensible, el bloqueo debe ser más estricto. También debe exigirse autenticación para desbloquear.

Contexto	Recomendación
Puesto administrativo común	Bloqueo automático por inactividad
Área financiera o datos sensibles	Tiempo de bloqueo más breve
Equipos compartidos	Cierre obligatorio de sesión al finalizar el uso
Celulares corporativos	PIN, contraseña o biometría
Trabajo remoto	Bloqueo obligatorio ante interrupciones

Ejemplo: un usuario deja una notebook abierta en una sala de reuniones. Si no existe bloqueo automático, otra persona podría leer correos, descargar archivos o realizar acciones en sistemas abiertos. Si el bloqueo se activa rápidamente, el riesgo disminuye.

9.8 Actualizaciones y gestión de parches

Las actualizaciones corrigen errores y vulnerabilidades. En los dispositivos finales deben cubrir el sistema operativo, navegadores, aplicaciones de oficina, clientes de correo, herramientas de videoconferencia, controladores, agentes de seguridad y aplicaciones específicas de negocio.

Las actualizaciones automáticas reducen el riesgo, pero deben ser gestionadas. En algunos entornos, instalar una actualización sin prueba puede afectar compatibilidad. En otros, demorarla demasiado deja expuesto al equipo.

Aspecto	Pregunta de gestión
Alcance	¿Qué aplicaciones deben actualizarse?
Frecuencia	¿Cada cuánto se verifica cumplimiento?
Criticidad	¿Qué parches deben aplicarse de inmediato?
Excepciones	¿Qué equipos no pueden actualizarse y por qué?

Aspecto	Pregunta de gestión
Evidencia	¿Cómo se demuestra que el equipo está actualizado?
Seguimiento	¿Qué ocurre con equipos que no reportan?

Ejemplo: una vulnerabilidad crítica afecta a un navegador utilizado por toda la empresa. Si el 95% de los equipos se actualiza en 48 horas, el riesgo se reduce. Si un 20% de equipos permanece sin actualizar durante semanas, la organización conserva una exposición innecesaria.

9.9 Antivirus, antimalware y EDR

La protección contra malware sigue siendo necesaria. El malware puede ingresar por correo, descargas, sitios comprometidos, dispositivos USB, aplicaciones falsas o vulnerabilidades. Las herramientas tradicionales de antivirus y antimalware detectan, bloquean o eliminan amenazas conocidas.

Las soluciones EDR agregan capacidades de detección y respuesta. No solo buscan archivos maliciosos, sino comportamientos sospechosos: procesos inusuales, cambios masivos de archivos, conexiones extrañas, intentos de elevación de privilegios o acciones compatibles con ransomware.

Control	Función principal	Limitación
Antivirus	Detecta amenazas conocidas	Puede fallar frente a ataques nuevos o comportamientos no identificados
Antimalware	Amplía detección de software malicioso	Requiere actualización y monitoreo

Control	Función principal	Limitación
EDR	Monitorea comportamiento y permite respuesta	Necesita análisis, procedimientos y responsables
Aislamiento de equipo	Evita propagación	Puede afectar operación si se aplica sin criterio
Recolección de evidencia	Apoya investigación	Requiere conservación adecuada

Ejemplo: una notebook comienza a modificar cientos de archivos en una carpeta compartida. Una herramienta EDR puede detectar el comportamiento, aislar el equipo y alertar al equipo de seguridad. Sin ese control, el incidente podría propagarse hacia otros dispositivos o respaldos conectados.

9.10 MDM y administración de dispositivos móviles

La administración de dispositivos móviles permite aplicar políticas sobre celulares, tabletas y, en algunos casos, notebooks. Su función es registrar dispositivos, configurar cuentas, exigir bloqueo, distribuir aplicaciones, controlar cumplimiento, separar datos personales y laborales, y ejecutar acciones como bloqueo o borrado remoto.

Función de MDM	Valor para la administración
Registro de dispositivos	Permite saber qué equipos acceden a información institucional
Políticas de bloqueo	Obliga a usar PIN, contraseña o biometría
Configuración de correo	Estandariza acceso seguro
Control de aplicaciones	Permite instalar o bloquear aplicaciones
Borrado remoto	Reduce exposición ante pérdida o robo

Función de MDM	Valor para la administración
Separación de datos	Ayuda en escenarios de dispositivos personales
Cumplimiento	Bloquea acceso si el dispositivo no cumple requisitos

Ejemplo: una organización define que todo celular con correo institucional debe tener bloqueo activo, sistema actualizado y posibilidad de borrado remoto. Si el dispositivo no cumple, se bloquea el acceso al correo corporativo. La herramienta técnica ejecuta una decisión administrativa previamente definida.

9.11 Control de USB y medios removibles

Los dispositivos USB permiten copiar datos, trasladar archivos, conectar periféricos o introducir software. También pueden ser una fuente de fuga de información o de ingreso de malware.

El control de USB no implica necesariamente prohibición absoluta. Debe definirse según el riesgo del área, la sensibilidad de los datos y la necesidad operativa.

Política posible	Uso recomendado
Bloqueo total de almacenamiento USB	Áreas con datos sensibles o alto riesgo
Permitir solo dispositivos autorizados	Procesos que necesitan intercambio físico controlado
Registrar uso de USB	Ambientes donde se requiere trazabilidad
Exigir cifrado en medios removibles	Transporte de información institucional
Autorizar excepciones temporales	Necesidades puntuales documentadas
Escaneo automático	Reducción del riesgo de malware

Ejemplo: el área de finanzas necesita entregar documentación digital a un tercero. La organización puede autorizar un dispositivo USB cifrado, asignarlo a un responsable, registrar los archivos copiados, establecer fecha de devolución y realizar borrado seguro luego de su uso.

9.12 BYOD: dispositivos personales en tareas laborales

BYOD se refiere al uso de dispositivos personales para acceder a recursos de la organización. Puede reducir costos y facilitar flexibilidad, pero aumenta los riesgos de seguridad, privacidad y soporte.

Riesgo BYOD	Implicancia administrativa
Dispositivo no administrado	La organización no conoce su estado de seguridad
Mezcla de datos personales y laborales	Se dificulta aplicar controles sin afectar privacidad
Uso compartido familiar	Terceros pueden acceder a datos institucionales
Falta de cifrado	Mayor exposición ante pérdida
Aplicaciones personales	Posible copia o sincronización no autorizada
Dificultad de borrado remoto	Conflicto entre datos personales y laborales
Falta de actualización	Exposición a vulnerabilidades conocidas

Una política BYOD debe definir qué dispositivos se permiten, qué sistemas pueden utilizar, qué requisitos mínimos deben cumplir, qué información puede descargarse, qué controles se aplican, qué soporte brinda la organización y qué ocurre ante pérdida, robo o desvinculación.

Ejemplo: un empleado accede a archivos de clientes desde una computadora personal compartida con familiares. Si no existe política BYOD, la organización no sabe si el equipo tiene cifrado, protección contra malware, bloqueo de sesión o almacenamiento seguro. La flexibilidad puede convertirse en exposición.

9.13 Trabajo remoto y seguridad del endpoint

El trabajo remoto amplía el perímetro de la organización. El usuario puede conectarse desde redes domésticas, espacios compartidos, hoteles, aulas, coworkings o redes públicas. En ese contexto, el endpoint debe tener controles propios, porque no siempre estará protegido por la red corporativa.

Control para trabajo remoto	Riesgo que reduce
Autenticación multifactor	Robo de contraseña
Acceso remoto seguro	Intercepción o acceso no autorizado
Dispositivo administrado	Falta de visibilidad sobre el equipo
Cifrado de disco	Exposición ante pérdida
Bloqueo de pantalla	Uso por terceros
Protección antimalware	Infección del equipo
Restricción de descargas	Copias locales no controladas
Capacitación específica	Conductas inseguras del usuario
Reporte inmediato de incidentes	Demora en la contención

El trabajo remoto debe regularse con una política clara. Debe indicar qué dispositivos están autorizados, qué aplicaciones se pueden usar, qué datos pueden descargarse, qué redes son aceptables, cómo se reportan incidentes y qué prácticas están prohibidas.

9.14 Privilegios locales y principio de mínimo privilegio

Los privilegios locales determinan qué puede hacer un usuario en su equipo. Una cuenta con permisos administrativos puede instalar software, modificar configuraciones, desactivar controles, crear usuarios, cambiar servicios y alterar componentes del sistema.

El principio de mínimo privilegio indica que cada usuario debe tener únicamente los permisos necesarios para cumplir su función. Los permisos administrativos permanentes aumentan el impacto de un error o de un malware.

Situación	Riesgo	Control recomendado
Usuario administrador permanente	Puede instalar software no autorizado	Quitar privilegios permanentes
Instalación ocasional necesaria	Se otorgan permisos excesivos	Usar elevación temporal aprobada
Malware ejecutado por usuario administrador	Mayor capacidad de daño	Aplicar mínimo privilegio
Técnicos con cuentas compartidas	Baja trazabilidad	Usar cuentas individuales
Cuentas locales antiguas	Acceso no controlado	Revisar y eliminar cuentas innecesarias

Ejemplo: un usuario administrativo descarga un archivo malicioso. Si su cuenta no tiene privilegios elevados, el daño puede limitarse. Si opera como administrador local, el malware puede modificar configuraciones, desactivar defensas e instalar componentes persistentes.

9.15 Software permitido, prohibido y control de aplicaciones

La organización debe definir qué software puede instalarse y ejecutarse. El software no autorizado puede introducir malware, incumplir licencias, copiar datos a terceros, generar incompatibilidades o afectar el rendimiento del equipo.

Categoría	Descripción
Software permitido	Aplicaciones aprobadas para uso institucional
Software prohibido	Aplicaciones no autorizadas por riesgo técnico, legal o de seguridad
Software restringido	Aplicaciones que requieren aprobación especial
Aplicaciones portables	Programas que se ejecutan sin instalación formal
Extensiones de navegador	Complementos que pueden acceder a datos o sesiones
Macros y scripts	Automatizaciones que pueden ejecutar código riesgoso

El control de aplicaciones permite limitar qué programas se ejecutan. Esto es importante porque algunas herramientas no necesitan instalación para operar. Un usuario puede ejecutar una aplicación portable desde una carpeta, un USB o una descarga.

Ejemplo: una extensión de navegador promete mejorar la productividad, pero solicita permiso para leer todas las páginas visitadas. Si el usuario accede a sistemas internos, la extensión podría capturar información sensible. Por eso, las extensiones también deben estar sujetas a control.

9.16 Datos locales y sincronización

Aunque la información principal esté en sistemas centrales o en la nube, los endpoints suelen almacenar copias locales. Los usuarios descargan archivos, generan reportes, exportan bases, sincronizan carpetas o guardan documentos en el escritorio. Esto crea riesgos de fuga, pérdida o duplicación.

Situación	Riesgo
Reporte descargado en escritorio	Queda fuera del repositorio controlado
Sincronización con cuenta personal	La información sale del dominio institucional
Exportación masiva	Mayor impacto ante robo o copia
Archivos temporales	Permanecen datos sensibles sin control
Carpetas no respaldadas	Pérdida de información relevante
Copias duplicadas	Dificultad para saber cuál es la versión válida

El endpoint debe ser considerado un lugar donde los datos están “en uso”. La seguridad no termina en el sistema central. Si una base de clientes se exporta a una planilla, la planilla pasa a ser un activo de información que requiere control.

9.17 Alta, reasignación, reparación y baja de dispositivos

La seguridad de endpoints debe cubrir todo el ciclo de vida del dispositivo. El riesgo no aparece solo durante el uso normal. También aparece cuando se compra, se configura, se entrega, se repara, se reasigna o se retira.

Etapa	Control necesario
Alta	Registro en inventario y configuración inicial segura
Asignación	Identificación del usuario responsable
Uso	Monitoreo, actualizaciones y cumplimiento de políticas

Etapa	Control necesario
Reparación	Cifrado, respaldo, retiro de datos o control del proveedor
Reasignación	Borrado seguro y reinstalación de imagen aprobada
Baja	Eliminación de datos, retiro del inventario activo y disposición segura

Ejemplo: una notebook devuelta por un empleado se entrega a otro usuario sin borrado seguro. El nuevo usuario puede acceder a archivos anteriores, correos descargados o configuraciones personales. La falla no está en el dispositivo, sino en el procedimiento administrativo.

Antes de enviar un equipo a reparación, deben cerrarse sesiones, retirar o cifrar almacenamiento, registrar la salida, verificar condiciones de confidencialidad del proveedor y revisar el equipo al retorno.

9.18 Borrado remoto y revocación de accesos

El borrado remoto permite eliminar información institucional de un dispositivo perdido, robado o fuera de control. Puede aplicarse a celulares, tabletas y notebooks administradas. En algunos casos borra todo el dispositivo; en otros, solo el contenedor corporativo.

El borrado remoto debe complementarse con otras acciones. Si un equipo se pierde, también deben revocarse sesiones, cambiar credenciales, bloquear tokens, revisar accesos recientes y documentar el incidente.

Acción	Finalidad
Bloquear dispositivo	Evitar nuevos accesos
Borrar información institucional	Reducir exposición de datos

Acción	Finalidad
Revocar sesiones	Impedir uso de sesiones abiertas
Cambiar credenciales	Reducir riesgo por claves guardadas
Revisar actividad reciente	Detectar uso indebido
Documentar incidente	Dejar evidencia para auditoría

El borrado remoto no reemplaza el cifrado. Si el dispositivo no vuelve a conectarse a Internet, la orden de borrado puede no ejecutarse de inmediato. Por eso, los controles deben ser acumulativos.

9.19 Capacitación de usuarios

La tecnología no reemplaza la conducta segura. Los usuarios deben conocer los riesgos básicos asociados al uso de dispositivos finales. La capacitación debe ser concreta, práctica y vinculada con situaciones cotidianas.

Tema de capacitación	Conducta esperada
Bloqueo de pantalla	Bloquear el equipo al ausentarse
Pérdida o robo	Reportar de inmediato
Correo sospechoso	No abrir enlaces ni adjuntos dudosos
Uso de USB	No conectar dispositivos desconocidos
Software	No instalar aplicaciones no autorizadas
Trabajo remoto	Usar solo canales permitidos
Datos sensibles	No descargar ni reenviar sin necesidad
Redes públicas	Evitar operaciones sensibles sin controles
Celulares	Usar bloqueo y no compartir el equipo

Tema de capacitación	Conducta esperada
Incidentes	Informar aunque parezcan menores

Ejemplo: si un usuario pierde un celular y espera varios días para avisar, el riesgo aumenta. La capacitación debe indicar que el reporte inmediato no busca sancionar al usuario, sino permitir contención rápida.

9.20 Indicadores de gestión

La seguridad de dispositivos finales debe medirse. Los indicadores permiten identificar brechas, justificar inversiones, priorizar controles y demostrar cumplimiento.

Indicador	Qué permite observar
Porcentaje de endpoints inventariados	Grado de visibilidad de activos
Porcentaje con cifrado activo	Protección ante pérdida o robo
Porcentaje con protección antimalware o EDR	Cobertura de defensa
Equipos sin reporte reciente	Dispositivos fuera de control
Equipos con parches críticos pendientes	Exposición a vulnerabilidades conocidas
Usuarios con privilegios locales	Riesgo por permisos excesivos
Incidentes de pérdida o robo	Nivel de exposición física
Uso de USB no autorizado	Intentos de extracción o conexión
Software prohibido detectado	Incumplimiento de política
Dispositivos BYOD registrados	Nivel de control sobre equipos personales

Un indicador aislado no siempre explica la situación completa. Por ejemplo, tener protección antimalware instalada no significa que todos los equipos estén protegidos si un porcentaje significativo no reporta actividad o tiene el agente desactualizado.

9.21 Respuesta ante incidentes en dispositivos finales

Los dispositivos finales pueden ser origen, medio o víctima de un incidente. La organización debe tener procedimientos específicos para pérdida, robo, malware, fuga de datos, software no autorizado, credenciales comprometidas y daño físico.

Incidente	Acciones iniciales
Pérdida de notebook	Bloquear equipo, revocar sesiones, evaluar datos locales y documentar
Robo de celular	Ejecutar borrado remoto, revocar tokens y revisar accesos recientes
Malware en endpoint	Aislar equipo, preservar evidencia, analizar alcance y restaurar
USB no autorizado	Registrar evento, analizar contenido y revisar posible fuga
Software prohibido	Remover aplicación, revisar actividad y reforzar controles
Credenciales comprometidas	Cambiar claves, cerrar sesiones y analizar accesos realizados

Ejemplo: una notebook muestra comportamiento compatible con ransomware. La acción inicial no debe ser seguir trabajando, sino aislar el equipo de la red, preservar evidencia, identificar archivos afectados, revisar si hubo propagación y restaurar desde una fuente confiable si corresponde.

9.22 Auditoría de seguridad de endpoints

La auditoría permite verificar si los controles existen, funcionan y dejan evidencia. No alcanza con preguntar si hay antivirus o si los usuarios “saben cuidarse”. Deben revisarse datos concretos.

Prueba de auditoría	Evidencia esperada
Selección de notebooks	Confirmación de cifrado, parches y protección activa
Comparación de inventario	Dispositivos activos contra registro formal
Revisión de privilegios	Listado de usuarios administradores locales
Control de software	Detección de aplicaciones no autorizadas
Verificación de MDM	Dispositivos móviles registrados y conformes
Revisión de incidentes	Procedimientos aplicados y tiempos de respuesta
Control de BYOD	Política, aceptación del usuario y cumplimiento técnico
Revisión de USB	Registros de conexión y excepciones autorizadas
Borrado remoto	Evidencia de prueba o ejecución
Baja y reasignación	Registros de borrado seguro y nueva entrega

Ejemplo de hallazgo: “Se identificaron 12 notebooks sin cifrado de disco. Cinco de ellas están asignadas a usuarios con acceso a información financiera”. La recomendación debe incluir cifrado obligatorio, bloqueo de acceso para equipos no conformes y seguimiento periódico.

9.23 Caso integrador: notebook perdida durante trabajo remoto

Una analista administrativa trabaja desde su domicilio con una notebook corporativa. El equipo contiene archivos descargados del sistema de proveedores y tiene acceso al correo institucional. Durante un traslado, la notebook se pierde.

Elemento	Análisis
Activo afectado	Notebook corporativa asignada a usuaria administrativa
Datos posibles	Archivos de proveedores, correos y documentos temporales
Riesgo principal	Acceso no autorizado a información institucional
Controles esperados	Cifrado, bloqueo, EDR, inventario, borrado remoto y revocación de sesiones
Acción inmediata	Reporte, bloqueo, revocación de accesos y análisis de actividad
Evaluación posterior	Determinar si había datos sensibles locales y si existió acceso posterior
Mejora	Reforzar política de descarga, capacitación y controles de sincronización

Este caso muestra que el incidente no se resuelve únicamente reemplazando el equipo. La organización debe evaluar información, credenciales, accesos, evidencia, obligaciones y mejoras de control.

9.24 Errores frecuentes

La seguridad de dispositivos finales suele fallar por problemas de gestión más que por falta de herramientas. Los errores más comunes son los siguientes:

Error	Consecuencia
No tener inventario completo	Equipos fuera de control
Permitir privilegios locales permanentes	Instalaciones y cambios no autorizados
No cifrar notebooks	Exposición de datos ante robo
Administrar celulares sin MDM	Falta de borrado remoto y control de cumplimiento
No revisar equipos sin reporte	Dispositivos desprotegidos
Permitir USB libremente	Riesgo de fuga o malware
No regular BYOD	Mezcla de datos personales y laborales
Reasignar equipos sin borrado seguro	Exposición de información anterior
Instalar herramientas sin monitoreo	Falsa sensación de seguridad
No capacitar usuarios	Conductas inseguras repetidas

La existencia de una herramienta no equivale a una gestión efectiva. Una organización puede tener EDR, MDM o antimalware y seguir expuesta si no revisa alertas, no mide cumplimiento o no corrige excepciones.

10 Ideas clave

10.1 Conceptos generales de seguridad

- **Security** se diferencia de **safety** porque se relaciona con amenazas intencionales, dinámicas y muchas veces externas a la organización.
- En TI, security se vincula con ciberseguridad, protección de datos, control de accesos, monitoreo, respuesta a incidentes y gestión de amenazas.
- La principal diferencia entre safety y security es la **intencionalidad**. Safety suele tratar fallas o accidentes. Security trata acciones deliberadas o maliciosas.

- Los datos históricos ayudan, pero en security no siempre predicen el futuro porque los atacantes cambian sus técnicas.
- La evaluación de riesgos de security suele requerir juicio experto, análisis cualitativo, escenarios, monitoreo y revisión continua.
- La mitigación es más compleja porque el atacante se adapta, aprende y busca debilidades técnicas, humanas o contractuales.
- La seguridad no debe tratarse como asunto exclusivamente técnico. Es un problema de gobierno, riesgo, estrategia y continuidad.
- Una organización segura no es la que nunca recibe ataques, sino la que puede prevenir, detectar, responder, recuperarse y aprender.
- En sistemas de información, security protege confidencialidad, integridad y disponibilidad.
- La dirección debe conocer indicadores de seguridad para tomar decisiones informadas sobre presupuesto, prioridades y riesgo residual.

10.2 Amenazas, vulnerabilidades y riesgo

- Una vulnerabilidad es una debilidad que puede ser aprovechada por una amenaza.
- La vulnerabilidad no es el daño ni la amenaza; es la condición que facilita el impacto.
- Las vulnerabilidades pueden ser técnicas, físicas, humanas, organizacionales o procedimentales.
- La complejidad no documentada aumenta la posibilidad de errores y controles incompletos.
- Los procedimientos computarizados relevantes deben auditarse y dejar evidencia.
- La continuidad operativa requiere limitar la extensión de los desastres.

- Las cuentas compartidas impiden saber quién realizó una acción.
- Identificación, autenticación y autorización son conceptos diferentes.
- Los controles de aplicación son esenciales para proteger procesos de negocio.
- La copia no autorizada de archivos puede ser difícil de detectar.
- Los cambios de código deben ser solicitados, probados, aprobados y documentados.
- La falta de reporte de errores agrava incidentes.
- Un bug es un defecto; un exploit es la forma de aprovechar una vulnerabilidad.
- La calidad de datos también forma parte de la seguridad de la información.
- La reducción de vulnerabilidades exige revisión periódica y mejora continua.

10.3 Mirada organizacional

- La seguridad de la información es una responsabilidad organizacional, no solo técnica.
- La estructura de roles define quién decide, quién ejecuta, quién controla y quién audita.
- El riesgo se administra mediante identificación, evaluación, tratamiento y seguimiento.
- La estrategia de seguridad debe alinearse con los objetivos del negocio.
- Las políticas deben ser claras, aplicables, comunicadas y revisadas.
- El cumplimiento normativo debe traducirse en controles concretos de TI.
- La gestión colaborativa exige coordinación, pero no elimina responsabilidades.

- La capacitación y la concientización cumplen funciones distintas y complementarias.
- La revocación inmediata de accesos ante desvinculaciones o transferencias es crítica.
- La separación de funciones reduce errores, fraudes y abusos.
- Las auditorías deben revisar evidencia verificable.
- El factor humano puede originar incidentes, pero también prevenirlos y detectarlos.
- Las formas de acceso deben modificarse cuando cambia el nivel de riesgo.

10.4 Gestión de activos

- Un activo de información es todo recurso físico, lógico, humano o documental que permite crear, procesar, almacenar, transmitir o proteger información relevante para la organización.
- La gestión de activos es la base de la seguridad, la auditoría, la continuidad y el control interno. No se puede proteger ni auditar lo que no se conoce.
- El inventario debe ser formal, actualizado y útil para la gestión. No debe limitarse a una lista estática de equipos.
- La clasificación de la información permite aplicar controles proporcionales al riesgo. No todos los datos requieren el mismo nivel de protección.
- El etiquetado transforma la clasificación en una práctica operativa, visible para usuarios y sistemas.
- Los roles de propietario, custodio y usuario ordenan la responsabilidad. TI no define por sí sola el valor funcional de los datos.

- El ciclo de vida de la información permite aplicar controles desde la creación hasta la destrucción segura.
- La retención documental debe equilibrar obligación legal, necesidad operativa y minimización del riesgo.
- El borrado simple no equivale a borrado seguro. La destrucción o eliminación debe impedir la recuperación de la información.
- Los soportes removibles deben ser inventariados, cifrados, controlados y destruidos adecuadamente al final de su vida útil.
- La nube y las aplicaciones SaaS amplían el alcance de la gestión de activos porque pueden crearse recursos fuera del entorno físico de la organización.
- La auditoría debe verificar evidencia: inventario, propietarios, clasificación, controles, retención, borrado y trazabilidad.

10.5 Políticas y gestión de accesos

- Las políticas administrativas de seguridad regulan comportamientos humanos frente a información, sistemas y accesos.
- Una política efectiva debe estar documentada, aprobada, comunicada, apoyada por controles técnicos y auditada.
- La política de escritorios limpios protege información física y documentos visibles.
- El bloqueo de pantalla protege sesiones activas frente a accesos locales no autorizados.
- La revocación de accesos ante la baja de usuarios debe ser completa y oportuna.
- La baja debe incluir sistemas internos, nube, VPN, correo, tokens, cuentas externas y credenciales físicas.

- Los cambios de función deben activar revisión de permisos.
- La acumulación gradual de privilegios viola el principio de mínimo privilegio.
- La recertificación periódica permite detectar accesos obsoletos o excesivos.
- Las cuentas inactivas deben bloquearse porque representan puntos de exposición.
- Bloquear y eliminar cuentas son acciones distintas.
- Las cuentas de servicio requieren inventario, responsable, permisos mínimos y revisión.
- Las políticas funcionan mejor cuando se integran al ciclo completo de vida del acceso.
- La comunicación, capacitación y cultura organizacional son esenciales.
- La conducta de los líderes influye en el cumplimiento real de las políticas.
- Las métricas permiten evaluar si una política funciona o solo existe en documentos.

10.6 Ingeniería social

- La ingeniería social explota **decisiones humanas dentro de procesos reales**, no fallas técnicas. Por eso, un sistema técnicamente bien configurado puede igualmente ser vulnerado si los procedimientos son débiles.
- El usuario no es externo al sistema de información: es parte de él. Su conducta —inducida o no— produce efectos reales sobre datos, operaciones y controles. Esto convierte la ingeniería social en un **riesgo de proceso**, no solo de personas.
- Los ataques más peligrosos son los más **personalizados**: el spear phishing al área de pagos o el vishing al soporte técnico son más efectivos que el phishing masivo porque generan confianza mediante datos reales.

- El **proceso de pagos** es uno de los más críticos: la modificación fraudulenta de un CBU puede generar pérdidas económicas inmediatas y mantener la obligación con el proveedor legítimo. La doble validación y el canal independiente son los controles más importantes en ese circuito.

- La **segregación de funciones** reduce el riesgo de fraude inducido porque ninguna persona puede completar sola todo el circuito de una operación sensible. Si una persona es manipulada, otra debe intervenir para que la acción se concrete.

- La **verificación por canal independiente** es el control más subestimado frente a la ingeniería social. Toda solicitud sensible debe confirmarse por un medio distinto al que llegó originalmente.

- Un **procedimiento informal** es una vulnerabilidad. Si una acción puede realizarse sin documentación, sin aprobación y sin evidencia, cualquier solicitud que imite el patrón habitual puede ser fraudulenta sin que nadie lo detecte.

- La **capacitación no es un evento puntual**: debe ser periódica, medible y orientada a casos reales. Las simulaciones internas permiten cuantificar la exposición y verificar si las acciones de mejora producen resultados.

10.7 Seguridad de los datos

- La seguridad de datos protege la información durante todo su ciclo de vida.

- Los datos son un activo central para operar, decidir y cumplir obligaciones.

- Confidencialidad, integridad y disponibilidad son pilares básicos, pero no suficientes por sí solos.

- La accesibilidad permite que los usuarios autorizados puedan usar los datos de manera oportuna y comprensible.

- La seguridad de datos no es responsabilidad exclusiva de TI; requiere participación de las áreas de negocio.

- Un dato puede ser técnicamente válido y administrativamente incorrecto.
- Los controles de entrada reducen errores en la captura inicial.
- Los controles de proceso verifican cálculos, transformaciones e integraciones.
- Los controles de salida protegen reportes, archivos y resultados.
- Las pistas de auditoría permiten reconstruir operaciones críticas.
- La integridad de mensajes protege archivos, transacciones y comunicaciones entre sistemas.
- La calidad de datos es parte de la seguridad porque sostiene decisiones confiables.
- GIGO recuerda que un sistema produce malos resultados si recibe datos deficientes.
- La clasificación de datos permite asignar controles proporcionales.
- Los backups deben probarse mediante restauraciones verificables.
- Los ambientes de prueba no deben exponer datos reales sin protección.
- El gobierno de datos ordena roles, definiciones, calidad, acceso y retención.

10.8 Bases de datos y analítica

- Las bases de datos concentran información crítica de la organización.
- La seguridad de bases de datos no se limita a contraseñas.
- El control de acceso debe definir usuarios, roles, permisos y condiciones.
- El principio de mínimo privilegio es central en bases de datos.
- Las vistas permiten mostrar solo los datos necesarios.
- Los stored procedures limitan operaciones y reducen exposición directa a tablas.

- La auditoría de consultas permite reconstruir accesos y cambios.
- El monitoreo de actividad permite detectar patrones anómalos.
- Los datos sensibles deben protegerse en producción, prueba, reportes, backups y analítica.
- Enmascaramiento, anonimización y seudonimización no son lo mismo.
- El DLP ayuda a prevenir fugas de información.
- La integridad referencial sostiene la consistencia de las relaciones entre datos.
- Los datos maestros requieren controles reforzados.
- Los sistemas de BI deben aplicar permisos por rol y registro de accesos.
- La exportación a hojas de cálculo es un riesgo frecuente de fuga.
- Los data lakes requieren clasificación, catálogo, linaje y gobierno.
- El gobierno de datos define responsabilidades sobre calidad, acceso, uso y retención.
- La seguridad de bases de datos está directamente vinculada con auditoría y cumplimiento.

10.9 Dispositivos finales

- Los dispositivos finales son activos de información porque permiten acceder, almacenar, procesar y transmitir datos institucionales.
- La seguridad de endpoints no depende solo del usuario. Requiere políticas, controles técnicos, procedimientos y evidencia.
- Las notebooks y celulares tienen riesgos particulares por su movilidad, uso fuera de la oficina y posibilidad de pérdida o robo.

- El inventario es la base de la gestión. No se puede proteger, actualizar ni auditar un dispositivo desconocido.
- El cifrado de disco reduce el impacto de pérdida o robo, pero debe combinarse con bloqueo, revocación de sesiones y borrado remoto.
- Las actualizaciones reducen exposición a vulnerabilidades conocidas, pero deben monitorearse con indicadores.
- MDM, EDR, antimalware, control de USB y control de aplicaciones son herramientas útiles, pero solo generan valor si están integradas a procesos de gestión.
- BYOD y trabajo remoto amplían el perímetro de riesgo y requieren reglas específicas.
- El principio de mínimo privilegio debe aplicarse también en los endpoints. Los usuarios no deberían tener permisos administrativos permanentes sin justificación.
- La auditoría de endpoints debe revisar evidencia real: inventario, cifrado, parches, privilegios, software, incidentes y cumplimiento de políticas.

11 Preguntas de evaluación

11.1 Conceptos generales de seguridad

- ¿Cuál es la diferencia principal entre safety y security?
- ¿Por qué la intencionalidad es un criterio central para distinguir ambos conceptos?
- ¿Cómo se aplica el concepto de security a las Tecnologías de la Información?
- ¿Por qué los datos históricos son menos confiables para predecir riesgos de security que riesgos de safety?
- ¿Qué significa que las amenazas de security sean dinámicas?

- ¿Por qué la evaluación del riesgo de security suele requerir opinión experta?
- ¿Qué diferencia existe entre un error de usuario y un ataque deliberado?
- ¿Cómo puede un proveedor tecnológico convertirse en fuente de riesgo de security?
- ¿Qué principios de la tríada CIA pueden verse afectados por un ataque de ransomware?
- ¿Por qué security debe ser considerada una cuestión estratégica y no solo técnica?
- ¿Qué indicadores debería revisar la dirección para conocer la madurez de seguridad de una organización?
- ¿Por qué la mitigación de security requiere controles preventivos, detectivos, correctivos y recuperatorios?
- ¿Qué errores frecuentes reducen la efectividad de la gestión de security?
- ¿Cómo se relacionan security y resiliencia organizacional?
- ¿Qué acciones mínimas debería implementar una organización para gestionar security en TI?

11.2 Amenazas, vulnerabilidades y riesgo

- ¿Qué diferencia existe entre una amenaza y una vulnerabilidad en un sistema de información?
- ¿Por qué las amenazas internas pueden ser tan relevantes como las amenazas externas?
- ¿Qué controles técnicos, administrativos y físicos podrían aplicarse para proteger un sistema de gestión?

- ¿Por qué la seguridad de la información debe analizarse desde la administración y no solo desde el área técnica?
- ¿Qué significa Defense in Depth (Defensa en profundidad) y por qué es importante?
- ¿Qué es una vulnerabilidad en un sistema de información?
- ¿Cuál es la diferencia entre amenaza, vulnerabilidad y riesgo?
- ¿Por qué la complejidad de los sistemas puede aumentar la exposición de una organización?
- ¿Qué riesgos generan los procedimientos computarizados no auditados?
- ¿Cómo puede extenderse el efecto de un desastre por falta de controles adecuados?
- ¿Cuál es la diferencia entre identificación, autenticación y autorización?
- ¿Por qué las cuentas compartidas generan problemas de trazabilidad?
- ¿Qué vulnerabilidades pueden surgir por modificaciones al código?
- ¿Por qué el personal de mantenimiento debe trabajar con procedimientos documentados?
- ¿Por qué los operadores deben reportar errores, alertas o anomalías?
- ¿Qué diferencia existe entre bug y exploit?
- ¿Cómo puede una filosofía de seguridad mal elegida generar vulnerabilidades?
- ¿Por qué la calidad de datos debe considerarse dentro de la seguridad de la información?
- ¿Qué controles pueden aplicarse para reducir el riesgo de copia no autorizada de archivos?

- ¿Por qué los backups deben probarse y no solo existir?
- ¿Qué vulnerabilidades pueden surgir por sistemas obsoletos o incompatibles?

11.3 Mirada organizacional

- ¿Por qué la seguridad de la información debe analizarse desde la organización y no solo desde el área técnica?
- ¿Qué relación existe entre seguridad, gobierno corporativo y control interno?
- ¿Qué roles deberían distinguirse en la gestión organizacional de la seguridad?
- ¿Cómo se administra un riesgo de seguridad de la información?
- ¿Qué elementos debería incluir una estrategia de seguridad?
- ¿Qué condiciones debe cumplir una política de seguridad para ser útil?
- ¿Cómo se traduce una obligación regulatoria en un control concreto de TI?
- ¿Por qué la gestión colaborativa no elimina responsabilidades individuales?
- ¿Cuál es la diferencia entre concientización y capacitación?
- ¿Por qué la revocación inmediata de privilegios es crítica ante una desvinculación?
- ¿Cómo contribuye la separación de funciones a reducir fraudes y errores?
- ¿Qué evidencias debería revisar una auditoría de seguridad?
- ¿Por qué los estándares deben adaptarse a cada organización?
- ¿Cómo puede el factor humano actuar como riesgo y como control?
- ¿Qué medidas pueden aplicarse para modificar formas de acceso ante nuevos riesgos?

- ¿Qué controles deberían aplicarse ante un cambio de cuenta bancaria de proveedor?

11.4 Gestión de activos

- ¿Qué es un activo de información y por qué su gestión no debe limitarse al inventario de equipos físicos?
- ¿Qué consecuencias administrativas puede generar un inventario de activos incompleto o desactualizado?
- ¿Qué información mínima debería contener el registro de un activo en el inventario institucional?
- ¿Cuál es la diferencia entre activo físico, activo lógico, activo de información, activo de software y activo en la nube?
- ¿Por qué una notebook perdida puede representar una brecha de seguridad aunque el valor económico del equipo sea bajo?
- ¿Qué diferencia existe entre clasificación y etiquetado de la información?
- ¿Cuáles son los cuatro niveles de clasificación más frecuentes y qué controles deberían aplicarse a la información confidencial?
- ¿Qué función cumple el propietario del activo y en qué se diferencia del custodio técnico?
- ¿Por qué el usuario de un activo no debería poder otorgar accesos a terceros sin autorización?
- ¿Cuáles son las etapas del ciclo de vida de la información y qué riesgos aparecen en cada una?
- ¿Por qué la retención documental no debe ser indefinida?

- ¿Qué riesgos genera conservar datos personales o información sensible más tiempo del necesario?
- ¿Por qué el simple borrado de un archivo no se considera borrado seguro?
- ¿En qué consiste la destrucción criptográfica y en qué situaciones puede ser útil?
- ¿Cuáles son los principales riesgos asociados a pendrives, discos externos y otros soportes removibles?
- ¿Qué controles deberían aplicarse a los soportes removibles utilizados en áreas administrativas o financieras?
- ¿Qué es la TI en la sombra y por qué puede afectar la gestión de activos en la nube?
- ¿Qué debería revisar una auditoría de TI sobre activos retirados de servicio?
- En el caso de la notebook perdida, ¿qué evidencia debería buscar la organización para determinar el impacto real?
- En el caso del sistema SaaS no registrado, ¿qué controles preventivos podrían haber evitado el riesgo?
- ¿Por qué la gestión de activos es una responsabilidad organizacional y no exclusivamente técnica?
- ¿Cómo se vincula la gestión de activos con la continuidad del negocio?
- ¿Qué indicadores podrían utilizarse para monitorear la madurez de la gestión de activos?
- ¿Qué hallazgos de auditoría podrían surgir de la ausencia de una política de retención documental?
- ¿Qué decisiones debería tomar la administración antes de destruir un activo que contiene información confidencial?

11.5 Políticas y gestión de accesos

- ¿Qué es una política administrativa de seguridad de la información?
- ¿Por qué una política escrita pero no aplicada no constituye un control efectivo?
- ¿Qué atributos debe tener una política de seguridad para ser eficaz?
- ¿Cómo se relacionan las políticas administrativas con los controles técnicos?
- ¿Qué establece la política de escritorios limpios?
- ¿Qué riesgos generan los documentos impresos visibles en escritorios?
- ¿Por qué las notas manuscritas también pueden representar riesgos de seguridad?
- ¿Por qué una pantalla desbloqueada equivale a un punto de acceso no autorizado?
- ¿Cómo debería implementarse el bloqueo automático de pantalla?
- ¿Qué métodos pueden usarse para verificar el cumplimiento de escritorios limpios?
- ¿Qué es el ciclo de vida del acceso?
- ¿Por qué la revocación de accesos al momento de la baja es un control crítico?
- ¿Qué accesos deben revocarse cuando una persona deja la organización?
- ¿Qué diferencia existe entre una baja parcial y una baja completa?
- ¿Por qué un cambio de función debe activar revisión de permisos?
- ¿Qué es la acumulación gradual de privilegios?
- ¿Qué establece el principio de mínimo privilegio?
- ¿Qué es la recertificación periódica de accesos?
- ¿Por qué una cuenta inactiva representa un riesgo?

- ¿Cuál es la diferencia entre bloquear y eliminar una cuenta?
- ¿Qué excepciones pueden existir frente al bloqueo por inactividad?
- ¿Qué son las cuentas de servicio y por qué requieren control especial?
- ¿Cómo se integran las políticas administrativas en el ciclo completo del acceso?
- ¿Qué documentación debe existir para que una política sea auditable?
- ¿Por qué la comunicación y la capacitación son necesarias para el cumplimiento?
- ¿Qué rol cumple la cultura organizacional en la efectividad de las políticas?
- ¿Por qué el comportamiento de los líderes influye en la seguridad?
- ¿Qué métricas pueden usarse para evaluar políticas administrativas de seguridad?
- ¿Qué evidencia debería existir ante una revocación de accesos?
- ¿Por qué la seguridad de la información debe entenderse como responsabilidad compartida?

11.6 Ingeniería social

- ¿Qué diferencia existe entre un ataque de ingeniería social y un ataque exclusivamente técnico? ¿Por qué esa diferencia cambia el tipo de control necesario?
- ¿Por qué el usuario es considerado parte del sistema de información y no un elemento externo? ¿Qué consecuencias tiene esa definición para la gestión del riesgo?
- ¿Cuál es la diferencia entre phishing, spear phishing, vishing y smishing en cuanto a canal, personalización y nivel de riesgo para cada tipo de organización?
- ¿Qué controles deberían aplicarse antes de autorizar la modificación de la cuenta bancaria de un proveedor? Describa el procedimiento paso a paso.

- ¿Por qué la segregación de funciones reduce el riesgo de fraude inducido por ingeniería social? Proporcione un ejemplo con el circuito de pagos.
- Un empleado del área de soporte recibe una llamada de alguien que dice ser el gerente de finanzas y solicita que le restablezca la contraseña de forma urgente porque está en una reunión. ¿Cómo debería responder el empleado y por qué?
- ¿Qué impacto puede tener el descarte inseguro de documentación? ¿Qué controles administrativos y físicos permiten reducirlo?
- Calcule el nivel de riesgo del spear phishing al área de pagos (probabilidad 3, impacto 5). ¿Qué tratamiento corresponde y qué controles específicos aplicaría?
- ¿Por qué los procedimientos informales aumentan el riesgo de ingeniería social? Proporcione un ejemplo concreto de cómo un procedimiento débil habilita un ataque.
- ¿Qué responsabilidades específicas debe asumir el área de administración —no solo el área técnica— en la prevención y respuesta ante ataques de ingeniería social?

11.7 Seguridad de los datos

- ¿Qué significa seguridad de datos desde la mirada de Tecnologías de la Información?
- ¿Cuál es la diferencia entre confidencialidad, integridad y disponibilidad?
- ¿Qué agrega el concepto de accesibilidad a la gestión de datos?
- ¿Por qué el acceso debe basarse en necesidad funcional?
- ¿Qué es la validación de datos y qué tipos de reglas puede incluir?
- ¿Qué función cumplen los controles de entrada?
- ¿Qué diferencia existe entre controles de entrada, proceso y salida?

- ¿Por qué son importantes los totales de control en procesos masivos?
- ¿Qué información debería registrar una pista de auditoría sobre un cambio crítico?
- ¿Qué es la integridad de mensajes y cómo puede verificarse?
- ¿Qué dimensiones forman parte de la calidad de datos?
- ¿Qué significa GIGO y por qué es importante para administración?
- ¿Por qué debe protegerse todo el ciclo de vida de los datos?
- ¿Qué criterios pueden usarse para clasificar datos?
- ¿Por qué un backup debe complementarse con pruebas de restauración?
- ¿Qué riesgos aparecen en integraciones y APIs?
- ¿Qué significa minimización de datos?
- ¿Por qué los ambientes de prueba pueden generar riesgos de seguridad?
- ¿Qué función cumple el gobierno de datos?
- ¿Qué métricas pueden ayudar a evaluar la seguridad y calidad de datos?

11.8 Bases de datos y analítica

- ¿Por qué una base de datos debe considerarse un activo organizacional crítico?
- ¿Qué función cumple un DBMS?
- ¿Cuál es la diferencia entre usuario de base de datos y rol de base de datos?
- ¿Por qué el principio de mínimo privilegio es especialmente importante en bases de datos?
- ¿Qué riesgo genera una aplicación con permisos de administrador sobre una base de datos?

- ¿Cómo puede una vista limitar el acceso a datos sensibles?
- ¿Qué es un stored procedure y para qué puede utilizarse como control?
- ¿Qué operaciones deberían registrarse en la auditoría de consultas?
- ¿Qué es el monitoreo de actividad de bases de datos?
- ¿Qué tipo de comportamiento anómalo debería generar una alerta?
- ¿Qué diferencia existe entre dato confidencial, sensible y crítico?
- ¿Qué es el enmascaramiento de datos?
- ¿Cuál es la diferencia entre enmascaramiento estático y dinámico?
- ¿Qué diferencia existe entre anonimización y seudonimización?
- ¿Por qué los datos seudonimizados siguen requiriendo protección?
- ¿Qué es DLP y en qué puntos puede operar?
- ¿Qué relación existe entre clasificación de datos y DLP?
- ¿Qué es la integridad referencial?
- ¿Por qué la falta de integridad referencial puede afectar la auditoría?
- ¿Qué son los datos maestros?
- ¿Por qué los cambios en CBU de proveedores deben tener controles reforzados?
- ¿Qué riesgos presentan los sistemas de BI?
- ¿Qué es RBAC y cómo se aplica en reportes?
- ¿Por qué exportar datos a hojas de cálculo puede generar fuga de información?
- ¿Qué riesgos específicos presentan los data lakes?

- ¿Qué es el gobierno de datos?
- ¿Cuál es la diferencia entre data owner, data steward y data custodian?
- ¿Qué función cumple un catálogo de datos?
- ¿Qué función cumple el linaje de datos?
- ¿Cómo se relaciona la seguridad de bases de datos con auditoría y cumplimiento?

11.9 Dispositivos finales

- ¿Qué es un dispositivo final y por qué debe ser tratado como un activo de información?
- ¿Por qué una notebook robada puede representar un riesgo mayor que la pérdida física del equipo?
- ¿Qué controles mínimos deberían aplicarse sobre notebooks utilizadas para trabajo administrativo?
- ¿Qué riesgos específicos presentan los celulares con correo institucional activo?
- ¿Qué información debería contener un inventario de dispositivos finales?
- ¿Por qué el cifrado de disco es un control esencial en equipos portátiles?
- ¿Qué diferencia existe entre antivirus tradicional y EDR?
- ¿Qué permite gestionar una herramienta MDM?
- ¿Por qué el uso de dispositivos USB debe regularse según el nivel de riesgo?
- ¿Qué significa BYOD y qué problemas administrativos genera?
- ¿Qué controles deberían exigirse para permitir trabajo remoto?
- ¿Por qué los privilegios locales permanentes aumentan el impacto de un incidente?

- ¿Qué diferencia existe entre software permitido, prohibido y restringido?
- ¿Por qué las extensiones de navegador deben ser consideradas dentro del control de aplicaciones?
- ¿Qué riesgos aparecen cuando los usuarios descargan datos locales desde sistemas centrales?
- ¿Qué controles deben aplicarse antes de reasignar una notebook a otro usuario?
- ¿Por qué el borrado remoto debe complementarse con revocación de sesiones?
- ¿Qué temas debería incluir una capacitación básica sobre seguridad de endpoints?
- ¿Qué indicadores usaría para presentar a la dirección el estado de seguridad de dispositivos finales?
- ¿Qué debería revisar una auditoría de seguridad de endpoints?
- En el caso de una notebook perdida, ¿qué acciones deberían realizarse durante las primeras horas?
- ¿Por qué la existencia de herramientas de seguridad no garantiza por sí sola una gestión efectiva?

12 Glosario de términos y siglas

Término	Explicación
Accesibilidad	Posibilidad de que las personas autorizadas usen los datos de manera razonable, oportuna y comprensible.
Access control	Control de acceso. Conjunto de medidas para definir quién puede ingresar a un sistema y qué puede hacer.

Término	Explicación
Access Management	Gestión de accesos. Proceso que controla el alta, modificación y baja de usuarios en los sistemas, incluyendo autorización formal y revisión periódica.
Access Point	Punto de acceso inalámbrico. Dispositivo que permite conectar equipos a una red Wi-Fi.
Active Directory	Servicio de directorio utilizado en entornos Windows para administrar usuarios, equipos y políticas.
Administración del riesgo (*risk management*)	Proceso sistemático para identificar, evaluar, tratar y monitorear riesgos.
Anonimización (*anonymization*)	Tratamiento que impide identificar a una persona a partir de los datos disponibles.
Antimalware	Herramienta destinada a detectar, bloquear o eliminar software malicioso.
Antivirus	Solución de seguridad orientada originalmente a detectar virus informáticos; actualmente suele incluir protección más amplia contra malware.
API (*Application Programming Interface*)	Interfaz de programación de aplicaciones. Permite que sistemas o aplicaciones se comuniquen entre sí.
Application controls	Controles de aplicación. Controles incorporados en sistemas de negocio para validar datos, limitar permisos, registrar operaciones y exigir aprobaciones.

Término	Explicación
Asset	Activo. Recurso con valor para la organización. En este contexto, recurso relacionado con información, sistemas o tecnología.
Asset Custodian	Custodio del activo. Persona o área que administra técnicamente un activo en nombre del propietario.
Asset Owner	Propietario del activo. Persona o área responsable funcional del activo, sus reglas de uso, clasificación y acceso.
Audit Log	Registro de auditoría. Registro cronológico e inmutable de acciones realizadas en un sistema: quién accedió, qué modificó y cuándo.
Audit trail	Pista de auditoría. Registro que permite reconstruir operaciones realizadas sobre datos o sistemas.
Auditoría	Revisión sistemática de controles, evidencias y cumplimiento de políticas o procedimientos.
Authentication	Autenticación. Verificación de la identidad de un usuario.
Authorization	Autorización. Asignación de permisos para definir qué puede hacer un usuario.
Availability	Disponibilidad. Propiedad que exige que los datos estén accesibles cuando se necesitan.
Awareness	Concientización. Toma de conciencia sobre riesgos y conductas esperadas.
Backup	Copia de respaldo. Copia de datos o sistemas destinada a permitir recuperación ante pérdida, daño o incidente.

Término	Explicación
Backups	Copias de respaldo utilizadas para recuperar información ante pérdida, daño, ransomware o interrupción.
Baiting	Cebo o señuelo. Técnica de ingeniería social que ofrece algo aparentemente atractivo (archivo, dispositivo, descarga) para inducir una conducta insegura.
BI (*Business Intelligence*)	Inteligencia de negocio. Sistemas y procesos que convierten datos en reportes, indicadores y análisis.
Bug	Error o defecto en el software, la lógica, la configuración o el comportamiento esperado de un programa.
Business continuity	Continuidad operativa. Capacidad de sostener o recuperar funciones críticas ante interrupciones.
BYOD	*Bring Your Own Device*. Uso de dispositivos personales para realizar tareas laborales o acceder a recursos institucionales.
CBU	Clave Bancaria Uniforme. Identificador bancario argentino de 22 dígitos que identifica una cuenta. Su modificación fraudulenta es uno de los vectores más frecuentes en ataques de ingeniería social en el circuito de pagos.
Change management	Gestión de cambios. Proceso para solicitar, aprobar, probar e implementar modificaciones en sistemas.
CIA (*Confidentiality, Integrity and Availability*)	*Confidentiality, Integrity and Availability*. Tríada que estructura los principios fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad.

Término	Explicación
Ciberseguridad	Conjunto de prácticas, tecnologías y procesos destinados a proteger sistemas, redes, datos y usuarios frente a amenazas digitales.
Cifrado de disco	Protección criptográfica de los datos almacenados en un dispositivo para que no puedan leerse sin autorización.
Clave foránea (*foreign key*)	Campo que relaciona una tabla con otra para mantener integridad referencial.
Clean desk policy	Política de escritorio limpio. Establece que documentos sensibles, contraseñas escritas y dispositivos removibles no deben quedar visibles o sin custodia en el puesto de trabajo.
Cloud Assets	Activos en la nube. Recursos tecnológicos contratados o gestionados en servicios externos de computación en la nube.
Confidentiality	Confidencialidad. Protección frente a accesos no autorizados.
Control compensatorio	Medida alternativa utilizada cuando no puede aplicarse el control ideal.
CRM (*Customer Relationship Management*)	*Customer Relationship Management*. Gestión de relaciones con clientes. Sistema utilizado para administrar información comercial, clientes, contactos y oportunidades.
Crypto Shredding	Destrucción criptográfica. Técnica que vuelve inaccesibles los datos cifrados eliminando la clave que permite descifrarlos.
DAM (*Database Activity Monitoring*)	Monitoreo de actividad de bases de datos. Herramientas que detectan accesos o consultas anómalas.

Término	Explicación
Data custodian	Custodio del dato. Área o persona responsable de implementar controles técnicos de almacenamiento, acceso y respaldo.
Data governance	Gobierno de datos. Conjunto de roles, políticas y controles para administrar datos como activos.
Data lake	Lago de datos. Repositorio que almacena grandes volúmenes de datos en formato original o poco transformado.
Data lineage	Linaje de datos. Trazabilidad del origen, transformación y destino de un dato.
Data Loss Prevention, DLP	Prevención de pérdida de datos. Conjunto de controles para evitar salidas no autorizadas de información.
Data masking	Enmascaramiento de datos. Sustitución de valores reales por valores ficticios para reducir exposición.
Data owner	Dueño del dato. Responsable funcional de definir reglas de uso, calidad, acceso y conservación.
Data quality	Calidad de datos. Grado de exactitud, consistencia, completitud y confiabilidad de la información.
Data steward	Administrador del dato. Responsable de calidad, definiciones y consistencia del dato.
DBMS (*Database Management System*)	Sistema de gestión de bases de datos. Permite almacenar, consultar, modificar, proteger y recuperar datos.
Defense in depth	Defensa en capas. Estrategia que utiliza varios niveles de control para reducir riesgos.

Término	Explicación
Degaussing	Desmagnetización. Proceso de eliminación de datos en medios magnéticos mediante campos magnéticos intensos.
DLP (*Data Loss Prevention*)	*Data Loss Prevention*. Prevención de pérdida de datos. Conjunto de controles para evitar fuga, copia o envío no autorizado de información sensible.
DoD 5220.22-M	Estándar históricamente asociado a métodos de sobrescritura segura de datos del Departamento de Defensa de los Estados Unidos.
Dueño del dato	Responsable funcional de definir el valor, uso permitido y nivel de protección de la información.
Dumpster Diving	Búsqueda en residuos físicos o digitales. Técnica que consiste en obtener información de documentos descartados, dispositivos obsoletos o soportes eliminados sin proceso seguro.
EDR	*Endpoint Detection and Response*. Detección y respuesta en dispositivos finales. Herramienta que monitorea endpoints, identifica comportamientos sospechosos y permite acciones de respuesta.
Encryption	Cifrado. Transformación de datos para impedir su lectura por personas no autorizadas.
Endpoint	Dispositivo final desde el cual un usuario accede a sistemas, datos o redes de la organización.
ERP (*Enterprise Resource Planning*)	*Enterprise Resource Planning*. Sistema de planificación de recursos empresariales. Integra en una única plataforma

Término	Explicación
	procesos como compras, ventas, inventarios, contabilidad y finanzas.
Exploit	Código, técnica o procedimiento que aprovecha una vulnerabilidad para producir un efecto no previsto.
Factor humano	Participación de las personas en el uso, administración, control y protección de la información.
Firewall	Cortafuegos. Dispositivo o software que controla el tráfico de red según reglas definidas.
Foreign key	Clave foránea. Relación técnica entre tablas de una base de datos.
Garbage In, Garbage Out, GIGO	"Basura entra, basura sale". Principio que indica que datos de entrada deficientes producen resultados deficientes.
GDPR / RGPD	*General Data Protection Regulation*. Reglamento General de Protección de Datos de la Unión Europea. Norma sobre protección de datos personales.
GPO (*Group Policy Object*)	Objeto de política de grupo. Herramienta utilizada para aplicar configuraciones centralizadas en entornos Windows.
Hardening	Endurecimiento de configuración. Proceso de reducir la superficie de ataque de un sistema mediante configuraciones seguras.
Hash	Huella digital calculada sobre datos para verificar si fueron alterados.

Término	Explicación
IAM (*Identity and Access Management*)	Gestión de identidades y accesos. Administración de usuarios, permisos, autenticación y ciclo de vida del acceso.
Identification	Identificación. Declaración de identidad de un usuario, por ejemplo mediante un nombre de usuario.
IDS	*Intrusion Detection System*. Sistema de detección de intrusiones. Herramienta que identifica actividad sospechosa o maliciosa.
Immutable backup	Copia de respaldo inmutable. Backup que no puede modificarse durante un período definido.
Information Technology, IT	Tecnologías de Información. En español se utiliza la sigla TI.
Input controls	Controles de entrada. Controles sobre los datos ingresados al sistema.
Integrity	Integridad. Propiedad que exige que los datos sean exactos, completos y no alterados indebidamente.
IP (*Internet Protocol*)	Protocolo de Internet. Identificador usado en redes para ubicar dispositivos o conexiones.
IPS	*Intrusion Prevention System*. Sistema de prevención de intrusiones. Herramienta que puede detectar y bloquear actividad maliciosa.
IRP	*Incident Response Plan*. Plan de respuesta a incidentes. Define los pasos para detectar, contener, analizar, comunicar,

Término	Explicación
	recuperar y documentar lecciones aprendidas ante un incidente de seguridad.
ISO 27001	Norma internacional para sistemas de gestión de seguridad de la información. Establece requisitos para gestionar riesgos y controles de seguridad.
IT (*Information Technology*)	*Information Technology*. Tecnologías de la Información (TI). Conjunto de recursos tecnológicos utilizados para procesar, almacenar, transmitir y proteger información.
LAN	*Local Area Network*. Red de área local. Red interna de una organización o sede.
Least privilege	Principio de mínimo privilegio. Establece que cada usuario debe tener acceso únicamente a los recursos necesarios para cumplir su función, sin permisos adicionales.
Malware	*Malicious Software*. Software malicioso diseñado para dañar, espiar, secuestrar, alterar o controlar sistemas sin autorización.
MDM	*Mobile Device Management*. Administración de dispositivos móviles. Permite gestionar celulares, tabletas y otros dispositivos mediante políticas centralizadas.
MFA (*Multi-Factor Authentication*)	*Multi-Factor Authentication*. Autenticación multifactor. Mecanismo que exige más de un factor de verificación para ingresar a un sistema: por ejemplo, contraseña más código temporal.
MFA, Multi-Factor Authentication	Autenticación multifactor. Método que exige más de un factor para comprobar la identidad.

Término	Explicación
Mínimo privilegio (*least privilege*)	Principio según el cual cada usuario debe tener solo los permisos necesarios para cumplir su función.
Offboarding	Proceso de baja o desvinculación. Incluye retirar accesos, recuperar equipos y cerrar responsabilidades.
Output controls	Controles de salida. Controles sobre reportes, archivos, consultas y resultados generados por el sistema.
PDF (*Portable Document Format*)	Formato de documento portable.
Phishing	Técnica de ingeniería social que consiste en enviar comunicaciones falsas que aparentan provenir de fuentes confiables para obtener credenciales, inducir descargas o forzar acciones.
PIN	*Personal Identification Number*. Número de identificación personal utilizado para desbloquear dispositivos o validar acceso.
Pretexting	Uso de pretexto. Técnica que construye una historia falsa y creíble (auditoría, urgencia de dirección, revisión de cuenta) para que la víctima actúe sin verificar.
Privilege creep	Acumulación gradual de privilegios. Situación en la que un usuario conserva permisos antiguos y suma nuevos accesos.
Privilegios	Permisos asignados a un usuario dentro de un sistema.
Processing controls	Controles de proceso. Controles aplicados durante el tratamiento, cálculo o transformación de datos.

Término	Explicación
Proxy	Servidor intermediario que gestiona solicitudes de usuarios hacia internet u otros servicios.
Pseudonymization	Seudonimización. Reemplazo de identificadores directos por referencias para reducir identificación directa.
Quid pro quo	Intercambio aparente. Técnica en la que el atacante ofrece asistencia, soporte o una ventaja a cambio de información o acceso. El engaño se presenta como colaboración.
Ransomware	Software malicioso que cifra archivos o sistemas y exige un pago para restaurar el acceso. En contextos de ingeniería social, suele instalarse después de que un usuario ejecuta un archivo engañoso.
RBAC (*Role-Based Access Control*)	Control de acceso basado en roles. Asigna permisos según el rol del usuario.
Recertificación de accesos	Revisión periódica en la que responsables funcionales confirman si los permisos siguen siendo necesarios.
Residual risk	Riesgo residual. Riesgo que permanece después de aplicar controles.
Resilience	Resiliencia. Capacidad de anticipar, resistir, responder y recuperarse ante eventos adversos.
Restore	Restauración. Proceso de recuperar datos desde una copia de respaldo.
Risk management	Gestión o administración del riesgo.

Término	Explicación
RPO (*Recovery Point Objective*)	Objetivo de punto de recuperación. Indica cuánta información puede perderse medida en tiempo.
RPO, Recovery Point Objective	Objetivo de punto de recuperación. Indica cuánta información puede perderse medida en tiempo.
RRHH / HR (*Human Resources*)	Recursos Humanos. Área responsable de gestionar altas, cambios, bajas y datos laborales.
RTO (*Recovery Time Objective*)	Objetivo de tiempo de recuperación. Indica cuánto tiempo puede estar caído un servicio.
RTO, Recovery Time Objective	Objetivo de tiempo de recuperación. Indica cuánto tiempo puede estar caído un servicio.
SaaS	*Software as a Service*. Software como servicio. Aplicación provista por un tercero y accedida normalmente por internet.
Safety	Seguridad operacional o protección frente a accidentes, fallas no maliciosas o riesgos conocidos de operación.
Security	Seguridad frente a amenazas intencionales, maliciosas, humanas, dinámicas o estratégicas. En TI, se asocia con ciberseguridad y protección de sistemas de información.
Security hole	Agujero de seguridad. Debilidad que puede permitir acceso, daño o uso indebido.
Segregation of duties	Separación de funciones. Distribución de tareas incompatibles entre distintas personas.
Service account	Cuenta de servicio. Cuenta utilizada por aplicaciones o procesos automatizados, no por una persona individual.

Término	Explicación
Shadow IT	TI en la sombra. Uso de sistemas, aplicaciones o servicios tecnológicos sin conocimiento o aprobación formal de TI.
SI	Sistema de Información. Combinación de personas, procesos, datos y tecnología orientada a producir información útil para la toma de decisiones.
SIEM	**Security Information and Event Management** (gestión de información y eventos de seguridad). Plataforma que centraliza registros y genera alertas.
SLA	*Service Level Agreement*. Acuerdo de nivel de servicio. Define compromisos medibles entre proveedor y cliente sobre disponibilidad, tiempos de respuesta y calidad del servicio.
Smishing	*SMS Phishing*. Variante de phishing que utiliza SMS o mensajería móvil para enviar enlaces falsos, alertas de seguridad falsas o instrucciones para instalar aplicaciones maliciosas.
Social Engineering	Ingeniería social. Conjunto de técnicas de manipulación psicológica orientadas a obtener de las personas información, acceso, autorizaciones o conductas útiles para el atacante.
SoD (*Segregation of Duties*)	*Segregation of Duties*. Segregación de funciones. Principio de control interno que evita que una misma persona concentre todas las etapas críticas de un proceso, reduciendo el riesgo de fraude.
Software permitido	Aplicaciones autorizadas por la organización para uso institucional.

Término	Explicación
Software prohibido	Aplicaciones no autorizadas por razones de seguridad, licenciamiento, privacidad o compatibilidad.
Spear Phishing	Phishing dirigido. Variante personalizada de phishing que utiliza información concreta sobre la víctima —cargo, proveedores, procesos— para aumentar la credibilidad del engaño.
SQL (*Structured Query Language*)	Lenguaje de consulta estructurada usado para consultar y administrar bases de datos relacionales.
SQL injection	Inyección SQL. Ataque que intenta insertar instrucciones SQL maliciosas en consultas o formularios.
Standards	Estándares o marcos de referencia que orientan buenas prácticas de gestión y control.
Stored procedure	Procedimiento almacenado. Bloque de instrucciones guardado en la base de datos para ejecutar operaciones definidas.
Switch	Dispositivo de red que conecta equipos dentro de una red local y dirige el tráfico entre ellos.
Tailgating	Ingreso físico por seguimiento. Técnica en la que una persona no autorizada accede a un área restringida siguiendo a alguien con acceso legítimo sin que nadie lo cuestione.
Término o sigla	Traducción / explicación
TI	Tecnologías de la Información (Information Technology). Área vinculada con sistemas, datos, infraestructura, redes, soporte y servicios tecnológicos.

Término	Explicación
TI / IT (*Information Technology*)	Tecnologías de la Información. Recursos tecnológicos utilizados para procesar, almacenar, transmitir y proteger información.
TI / IT, Information Technology	Tecnologías de la Información. Conjunto de recursos tecnológicos utilizados para procesar, almacenar, transmitir y proteger información.
Token	Elemento digital utilizado para mantener una sesión o validar una autenticación. Si se compromete, puede permitir acceso indebido.
Training	Capacitación. Formación orientada a desarrollar habilidades concretas.
UPS	*Uninterruptible Power Supply*. Sistema de alimentación ininterrumpida. Equipo que mantiene energía temporalmente ante cortes eléctricos.
USB (*Universal Serial Bus*)	*Universal Serial Bus*. Puerto de conexión estándar en equipos informáticos. Los dispositivos USB (memorias, discos externos) son un vector frecuente de ataques de tipo baiting.
Validación de datos	Verificación de que los datos cumplen reglas de formato, rango, consistencia, obligatoriedad o negocio.
View	Vista. Consulta predefinida que muestra un subconjunto de datos sin dar acceso directo a las tablas originales.
Vishing	*Voice Phishing*. Variante de phishing que se realiza mediante llamadas telefónicas. El atacante suplanta la identidad de

Término	Explicación
	soporte técnico, auditoría, proveedores o directivos para obtener datos o acceso.
VPN (*Virtual Private Network*)	*Virtual Private Network*. Red privada virtual. Canal cifrado para conectar usuarios o sedes a recursos internos mediante redes no confiables como internet.
Vulnerabilidad	Debilidad que puede ser explotada por una amenaza para afectar un activo.
Vulnerability	Vulnerabilidad. Debilidad técnica, física, humana, organizacional o procedimental que puede ser aprovechada por una amenaza.
Walk-through	Recorrida física o recorrido de verificación. Técnica para observar el cumplimiento de controles en el lugar.
WLAN	*Wireless Local Area Network*. Red de área local inalámbrica. Red Wi-Fi utilizada dentro de una organización o espacio determinado.
Zero Trust	Modelo de seguridad basado en no confiar automáticamente en usuarios, dispositivos o redes, y verificar cada acceso según identidad, contexto y riesgo.