Conceptos Generales de Seguridad de la información y administración de Tecnologías de Información

1.1 Seguridad de la información como problema de gestión

La seguridad de la información no debe entenderse únicamente como un conjunto de herramientas técnicas. En una organización, la información permite vender, comprar, pagar, cobrar, liquidar sueldos, facturar, administrar contratos, registrar operaciones, atender clientes, cumplir obligaciones legales y tomar decisiones. Por ese motivo, protegerla forma parte de la administración general de la organización.

Desde la perspectiva de Tecnologías de Información, la seguridad busca preservar tres propiedades básicas: confidencialidad, integridad y disponibilidad. La confidencialidad implica que la información solo sea conocida por quienes están autorizados. La integridad significa que los datos se mantengan completos, correctos y no alterados indebidamente. La disponibilidad exige que los sistemas y datos estén accesibles cuando los procesos de negocio los necesitan.

Propiedad	Pregunta administrativa	Ejemplo de riesgo
Confidencialidad	¿Quién puede ver la información?	Exposición de datos de clientes o empleados.
Integridad	¿La información es correcta y no fue modificada sin autorización?	Alteración de una cuenta bancaria de proveedor.
Disponibilidad	¿El sistema está operativo cuando se lo necesita?	Caída del sistema de facturación durante el cierre mensual.

La seguridad tiene impacto directo sobre el control interno. Un sistema puede estar técnicamente funcionando, pero ser administrativamente riesgoso si permite accesos

excesivos, no registra cambios, no conserva evidencia o no permite reconstruir quién hizo qué. Por eso, la seguridad se relaciona con la contabilidad, la auditoría, los contratos, la gestión de personas, la continuidad del negocio y la responsabilidad de la dirección.

En clase se destacó una idea central: la seguridad no consiste en evitar todo riesgo, porque eso no es posible ni económicamente razonable. Consiste en identificar los riesgos relevantes, priorizarlos, aplicar controles proporcionales, registrar decisiones y revisar resultados. Una organización debe saber qué activos son críticos, qué datos requieren mayor protección, qué incidentes podrían interrumpir la operación y qué nivel de pérdida o interrupción puede tolerar.

1.1.1 De lo técnico a lo administrativo

Un problema técnico se convierte en un problema administrativo cuando afecta un proceso de negocio. Por ejemplo, una contraseña débil puede parecer un detalle menor. Sin embargo, si esa contraseña permite ingresar al sistema de pagos, el riesgo deja de ser técnico y se convierte en un riesgo financiero. Del mismo modo, una base de datos sin cifrado puede afectar obligaciones legales, contratos, reputación y relación con clientes.

La administración debe traducir los riesgos de TI en preguntas de gestión:

Pregunta de gestión	Sentido práctico
¿Qué proceso se afecta?	Permite medir impacto operativo.
¿Qué datos están involucrados?	Permite evaluar confidencialidad, integridad y cumplimiento.
¿Quién es responsable del activo?	Permite asignar decisiones y controles.
¿Qué evidencia queda?	Permite auditar, investigar y defender decisiones.
¿Qué plazo de recuperación se necesita?	Permite definir continuidad del negocio.

Pregunta de gestión	Sentido práctico
¿Qué proveedor participa?	Permite evaluar contratos y responsabilidad de terceros.

La seguridad, por lo tanto, no puede quedar limitada al área técnica. El área de TI administra infraestructura y sistemas, pero las áreas de negocio conocen el valor de los datos y las consecuencias operativas de una interrupción o error. La dirección debe definir prioridades, aprobar políticas, asignar presupuesto y exigir evidencia.

1.1.2 Ideas clave

- La seguridad de la información es parte del gobierno organizacional.
- Confidencialidad, integridad y disponibilidad son propiedades básicas, pero deben traducirse a procesos concretos.
- Un riesgo técnico puede generar consecuencias económicas, legales, operativas y reputacionales.
- La administración debe exigir responsables, criterios de decisión, controles, evidencia y revisión.
- No todo activo requiere el mismo nivel de protección; la prioridad depende del impacto.

1.2 Gobierno de la seguridad de la información

El gobierno de la seguridad de la información es el conjunto de responsabilidades, políticas, decisiones, controles, indicadores y mecanismos de rendición de cuentas mediante los cuales una organización dirige y supervisa la protección de su información.

Gobernar la seguridad implica responder preguntas concretas: quién decide, quién ejecuta, quién controla, quién informa, quién acepta riesgos y quién responde ante incidentes. Cuando esas respuestas no están definidas, la organización puede tener herramientas, pero no necesariamente una gestión segura.

Una política de seguridad puede exigir autenticación multifactor, pero si nadie revisa su cumplimiento, el control queda debilitado. Un área puede tener respaldos, pero si nunca se prueban restauraciones, no se sabe si realmente sirven. Un proveedor puede prometer seguridad, pero sin cláusulas contractuales, auditoría y seguimiento, esa promesa resulta difícil de verificar.

1.2.1 Seguridad como función de dirección

La alta gerencia no necesita administrar firewalls ni configurar servidores. Su responsabilidad es distinta: definir criterios, aprobar políticas, revisar indicadores, asignar recursos y exigir evidencia. La seguridad debe formar parte del tablero de gestión, igual que los indicadores financieros, comerciales o de operaciones.

Ejemplo: si el canal digital representa una parte relevante de los ingresos, la dirección debe conocer el nivel de disponibilidad requerido, los tiempos de recuperación, los controles de acceso, los riesgos de proveedores y la capacidad de respuesta ante incidentes. No basta con suponer que “TI se ocupa”.

1.2.2 Roles principales

Rol	Función principal	Riesgo si no existe
Alta gerencia o directorio	Define prioridades, apetito de riesgo y recursos.	Seguridad sin respaldo institucional.
Responsable de seguridad o CISO	Coordina políticas, controles, riesgos e informes.	Controles dispersos y sin seguimiento.
Comité de seguridad	Integra TI, negocio, legales, auditoría y dirección.	Decisiones aisladas o contradictorias.
Propietario del activo	Define valor, criticidad y reglas de acceso.	Sistemas sin dueño funcional.

Rol	Función principal	Riesgo si no existe
Responsable del proceso	Integra seguridad al circuito operativo.	Controles técnicos desconectados de la operación.
Auditoría	Revisa evidencia y cumplimiento.	Declaraciones sin verificación independiente.

El responsable de seguridad debe traducir lenguaje técnico a lenguaje ejecutivo. No alcanza con informar que hubo eventos o alertas. Debe explicarse qué riesgo existe, qué activos se afectan, qué impacto podría producirse, qué acciones se tomaron y qué decisión se requiere.

1.2.3 Matriz RACI

La matriz RACI ayuda a ordenar responsabilidades. RACI significa Responsible, Accountable, Consulted, Informed. En español puede entenderse como: responsable de ejecutar, responsable final, consultado e informado.

Ejemplo aplicado a la baja de usuarios:

Actividad	RR. HH.	Jefatura	TI	Seguridad	Auditoría
Informar desvinculación	R	C	I	I	I
Validar accesos asociados	C	R	C	I	I
Ejecutar baja técnica	I	I	R	C	I
Verificar cumplimiento	I	I	C	A	I
Revisar evidencia periódica	I	I	I	C	R

La matriz evita ambigüedades. Si no se sabe quién debe aprobar un acceso, quién debe darlo de baja o quién debe revisar evidencia, el proceso termina dependiendo de personas y no de reglas institucionales.

1.2.4 Políticas, normas, procedimientos y evidencias

El gobierno de seguridad requiere documentación en niveles. La política define principios generales. Las normas establecen reglas obligatorias. Los procedimientos describen pasos. Los instructivos explican tareas específicas. Las evidencias demuestran que el control fue ejecutado.

Nivel documental	Ejemplo
Política	Todo acceso a sistemas críticos debe estar autorizado.
Norma	Los accesos privilegiados deben usar MFA y revisarse mensualmente.
Procedimiento	Solicitud, aprobación, alta, revisión y baja de usuarios.
Instructivo	Pasos concretos para desactivar un usuario en cada plataforma.
Evidencia	Ticket, aprobación, registro de baja, reporte revisado.

Sin evidencia, la organización solo declara intenciones. La evidencia permite auditar, investigar incidentes, responder ante reclamos y mejorar procesos.

1.2.5 NIST CSF como referencia

Un marco útil para ordenar la seguridad es el NIST Cybersecurity Framework. Este marco organiza la gestión en funciones: gobernar, identificar, proteger, detectar, responder y recuperar.

Función	Pregunta central	Ejemplo de actividad
Gobernar	¿Quién decide y con qué criterios?	Política, roles, comité, riesgos.
Identificar	¿Qué activos, datos y riesgos existen?	Inventario, clasificación, mapa de procesos.

Función	Pregunta central	Ejemplo de actividad
Proteger	¿Qué controles reducen el riesgo?	MFA, cifrado, backups, capacitación.
Detectar	¿Cómo se descubren eventos anómalos?	Logs, alertas, monitoreo, revisión de accesos.
Responder	¿Cómo se actúa ante incidentes?	Contención, comunicación, evidencia.
Recuperar	¿Cómo se vuelve a operar?	Restauración, continuidad, lecciones aprendidas.

Este marco ayuda a evitar una visión parcial. Una organización puede proteger, pero no detectar. Puede detectar, pero no responder. Puede tener backups, pero no haber probado recuperación. La seguridad requiere equilibrio entre todas las funciones.

1.2.6 Indicadores de gestión

La seguridad debe medirse. Algunos indicadores útiles para la administración son:

Indicador	Qué permite evaluar
Porcentaje de sistemas críticos con MFA	Madurez de control de accesos.
Tiempo promedio de baja de usuarios	Riesgo por accesos residuales.
Vulnerabilidades críticas abiertas	Exposición técnica relevante.
Porcentaje de restauraciones probadas	Capacidad real de recuperación.
Incidentes por severidad	Evolución del riesgo operativo.
Proveedores críticos evaluados	Gestión de riesgo de terceros.
Usuarios capacitados	Cobertura de concientización.

Un indicador debe tener fórmula, responsable, fuente, frecuencia y umbral. Si el indicador no genera decisiones, se convierte en una medición decorativa.

1.2.7 Ideas clave

- El gobierno de seguridad define responsabilidades, criterios y rendición de cuentas.
- La alta gerencia debe supervisar riesgos, no solo aprobar herramientas.
- Las políticas necesitan procedimientos y evidencias.
- La matriz RACI evita confusión de roles.
- Los indicadores permiten convertir seguridad en gestión medible.

1.3 Comunicaciones e Internet

La seguridad de las comunicaciones protege los datos cuando se transmiten entre personas, sistemas, aplicaciones, redes, proveedores, clientes y servicios externos. Una organización puede tener bases de datos protegidas y, al mismo tiempo, exponer información si sus comunicaciones son débiles.

Cada comunicación tiene origen, destino, canal, contenido, protocolo, permisos y registro. El riesgo aparece cuando esa comunicación puede ser leída, alterada, bloqueada, suplantada o reutilizada por terceros no autorizados.

Ejemplo: si una sucursal transmite archivos de ventas al sistema central y el archivo llega incompleto o alterado, el problema afecta facturación, stock y conciliación. Si no se sabe quién envió el archivo, la auditoría tendrá dificultades para reconstruir el proceso.

1.3.1 Controles sobre comunicaciones

Tipo de control	Finalidad	Ejemplo
Preventivo	Evitar lectura o alteración indebida.	Cifrado, VPN, certificados, firewalls.

Tipo de control	Finalidad	Ejemplo
Detectivo	Identificar anomalías o errores.	Logs, alertas, IDS, conciliaciones.
Correctivo	Corregir configuraciones o accesos.	Revocar certificados, bloquear direcciones.
Recuperatorio	Restaurar servicios o canales.	Enlaces alternativos, contingencia.

La comunicación segura no se limita a cifrar. También requiere autenticar a las partes, validar mensajes, controlar integridad, registrar eventos y definir procedimientos ante errores.

1.3.2 Validación de datos transmitidos

En procesos administrativos, un mensaje técnicamente entregado puede ser inválido si no cumple reglas de negocio. Por eso, la validación debe incluir formato, origen, destino, fecha, secuencia, cantidad de registros, totales, hash, firma o aprobación.

Ejemplo: un archivo de pagos contiene 1.200 operaciones por un total de 80 millones de pesos. Si el sistema receptor registra 1.198 operaciones por 79,85 millones, existe una disparidad que debe investigarse. No corresponde cerrar el proceso sin revisar logs, archivo original, integridad y reportes de importación.

Control	Uso
Conteo de registros	Verifica cantidad de operaciones.
Total de control	Compara montos esperados y recibidos.
Número de secuencia	Evita duplicados u omisiones.
Hash	Detecta cambios en el archivo.

Control	Uso
Firma digital	Verifica integridad y autoría.
Acuse de recibo	Confirma recepción formal.

1.3.3 Cifrado, TLS y certificados

El cifrado transforma información para que no pueda ser leída sin una clave. En comunicaciones, protege la confidencialidad. TLS es el protocolo usado para proteger muchas conexiones en Internet, especialmente HTTPS.

Sin embargo, "tener HTTPS" no es suficiente. Deben usarse versiones vigentes, certificados válidos, algoritmos seguros, renovación oportuna y monitoreo de vencimientos. Un certificado vencido puede interrumpir el acceso de clientes o usuarios. Una configuración débil puede permitir ataques contra la comunicación.

El certificado digital vincula una clave pública con una identidad. Permite verificar que el servidor o entidad con la que se comunica el usuario es quien dice ser. En comunicaciones entre sistemas puede usarse mTLS, donde tanto cliente como servidor presentan certificados.

1.3.4 Firma digital e integridad

La firma digital permite verificar autoría e integridad de un documento o mensaje. No debe confundirse con una imagen de firma manuscrita. Una imagen puede copiarse y pegarse; una firma digital permite detectar si el archivo fue modificado luego de firmado.

En administración, la firma digital tiene valor para contratos, aprobaciones, órdenes, facturas, comunicaciones formales y archivos críticos. También ayuda a resolver controversias: si un archivo se modifica después de la firma, la verificación falla.

1.3.5 VPN, ZTNA y acceso remoto

La VPN crea un canal cifrado entre el dispositivo del usuario y la red de la organización. Es útil para acceso remoto, comunicación entre sedes y soporte de proveedores. Pero no

equivale a seguridad completa. Si el usuario tiene credenciales comprometidas o el dispositivo está infectado, la VPN puede convertirse en una vía de ingreso.

La tendencia actual es limitar el acceso. En lugar de permitir entrada a toda la red, se procura otorgar acceso solo a la aplicación o recurso necesario, por el tiempo necesario y con registro de actividad. Ese enfoque se asocia con ZTNA, acceso de red con enfoque de confianza cero.

Ejemplo: un proveedor necesita ingresar durante dos horas a un servidor específico. La organización puede otorgar acceso temporal, con MFA, solo a ese servidor y con registro. Esto es más seguro que mantener una VPN permanente con acceso amplio.

1.3.6 Seguridad del DNS y dominios

El DNS traduce nombres de dominio en direcciones de red. Si falla o se manipula, los usuarios pueden ser enviados a destinos incorrectos. Un dominio vencido puede interrumpir correo, sitio web, aplicaciones y servicios asociados.

La administración debe tener responsables para dominios, certificados, cambios DNS y vencimientos. Los cambios críticos deben requerir doble aprobación y quedar registrados.

1.3.7 Ideas clave

- Las comunicaciones deben proteger confidencialidad, integridad, autenticación y disponibilidad.
- Un archivo recibido puede ser técnicamente correcto pero administrativamente inválido.
- La firma digital protege autoría e integridad, no es una imagen de firma.
- VPN debe combinarse con MFA, segmentación y permisos mínimos.
- DNS, certificados y dominios requieren gestión administrativa, no solo técnica.

1.4 Seguridad de redes moderna

La red es la infraestructura que permite la comunicación entre usuarios, aplicaciones, sistemas internos, proveedores, servicios en la nube e Internet. Una red sin controles adecuados expone simultáneamente a todos los sistemas conectados.

El modelo tradicional confiaba en un perímetro: lo interno era considerado confiable y lo externo no. Ese modelo resulta insuficiente. Hoy los usuarios trabajan desde distintos lugares, los sistemas están en la nube, los proveedores se conectan remotamente y los atacantes buscan moverse lateralmente dentro de la red.

1.4.1 Arquitectura de red segura

Una arquitectura segura organiza zonas, controla tráfico y aplica defensa en profundidad. Defensa en profundidad significa usar varias capas de control para que la falla de una no comprometa todo el entorno.

El principio clave es la segmentación. Los sistemas financieros no deberían estar en el mismo segmento que los equipos de uso general. Las bases de datos no deberían ser accesibles directamente desde la red de usuarios. Los dispositivos de invitados no deberían comunicarse con servidores internos.

Zona	Riesgo principal	Control esperado
Usuarios internos	Malware, credenciales comprometidas.	Segmentación, EDR, mínimo privilegio.
Servidores críticos	Alteración o indisponibilidad de procesos.	Firewalls internos, monitoreo, acceso restringido.
DMZ	Exposición a Internet.	Reglas estrictas hacia red interna.

Zona	Riesgo principal	Control esperado
Invitados	Dispositivos no controlados.	Aislamiento completo de red corporativa.
IoT	Equipos con baja seguridad.	VLAN separada y restricciones.

La DMZ es una zona intermedia para sistemas expuestos a Internet, como portales web o servicios públicos. Si un sistema en la DMZ es comprometido, el atacante no debería poder avanzar libremente hacia la red interna.

1.4.2 Firewalls, IDS, IPS y WAF

El firewall controla tráfico según reglas. Puede permitir o bloquear conexiones por origen, destino, puerto, protocolo o aplicación. Es básico, pero no suficiente.

El IDS detecta tráfico sospechoso y genera alertas. El IPS puede bloquearlo. El WAF protege aplicaciones web analizando solicitudes HTTP o HTTPS para detectar ataques como inyección SQL o abuso de formularios.

Control	Función	Ejemplo
Firewall	Filtra tráfico de red.	Bloquear accesos no autorizados.
IDS	Detecta intrusiones.	Alertar sobre patrón sospechoso.
IPS	Detecta y bloquea.	Interrumpir tráfico malicioso.
WAF	Protege aplicaciones web.	Bloquear inyección SQL.

El firewall de red puede permitir tráfico HTTPS porque el puerto está habilitado. El WAF analiza el contenido de la solicitud y puede detectar que un parámetro contiene instrucciones maliciosas.

1.4.3 Proxy, Secure Web Gateway y DNS seguro

El proxy actúa como intermediario entre usuarios e Internet. Permite aplicar políticas de navegación, registrar accesos y bloquear destinos. El Secure Web Gateway agrega capacidades como análisis de malware, reputación de sitios, inspección de tráfico y políticas de uso aceptable.

El DNS seguro bloquea dominios maliciosos antes de que el usuario establezca conexión. Es un control temprano y útil para reducir exposición a sitios usados para phishing, malware o comunicaciones de comando y control.

1.4.4 NAC y control de dispositivos

El NAC verifica el estado de un dispositivo antes de permitirle acceder a la red. Puede revisar si el sistema operativo está actualizado, si tiene protección activa, si está cifrado o si pertenece al inventario corporativo. Si no cumple, puede ponerlo en cuarentena.

Ejemplo: un consultor conecta su notebook personal a la red. El NAC detecta que no tiene antivirus activo ni actualizaciones recientes y lo ubica en una VLAN de cuarentena sin acceso a recursos internos.

1.4.5 Zero Trust

Zero Trust significa confianza cero. No implica desconfiar culturalmente de las personas, sino no asumir que una red interna es segura por sí misma. Cada acceso debe verificarse según identidad, dispositivo, contexto, recurso y nivel de riesgo.

Principios operativos:

Principio	Significado
Verificar siempre	No confiar por ubicación o red de origen.
Mínimo privilegio	Otorgar solo el acceso necesario.

Principio	Significado
Asumir compromiso	Diseñar controles como si algún componente ya pudiera estar comprometido.

Implementar Zero Trust no consiste en comprar un producto. Requiere inventario, clasificación de aplicaciones, identidad fuerte, MFA, monitoreo, segmentación y revisión de permisos.

1.4.6 Wi-Fi, routers y switches

La red inalámbrica debe separarse por uso: corporativa, invitados, dispositivos personales o IoT. La red de invitados no debe acceder a sistemas internos. Las redes nuevas deberían usar WPA3 cuando sea posible.

Routers y switches también requieren hardening: cambiar credenciales por defecto, usar protocolos seguros, actualizar firmware, restringir acceso de administración y revisar configuraciones. Un switch comprometido puede permitir redireccionar tráfico, capturar comunicaciones o alterar segmentación.

1.4.7 Ideas clave

- La red no debe ser plana; debe estar segmentada.
- La DMZ limita el impacto de sistemas expuestos a Internet.
- Firewall, IDS, IPS y WAF cumplen funciones distintas.
- Zero Trust verifica accesos por identidad, dispositivo, contexto y riesgo.
- Los dispositivos de red también son activos críticos y deben endurecerse.

1.5 Seguridad en la nube

La computación en la nube permitió contratar infraestructura, plataformas y aplicaciones como servicios escalables. Pero la contratación de un servicio en la nube no elimina la responsabilidad de la organización sobre sus datos, usuarios, configuraciones y procesos.

El error más frecuente es creer que "la seguridad queda a cargo del proveedor". En realidad, la responsabilidad se redistribuye. El proveedor protege la infraestructura que opera; la organización protege cómo usa el servicio.

1.5.1 Modelos de servicio

Modelo	Qué ofrece	Qué gestiona principalmente la organización
IaaS	Servidores virtuales, redes y almacenamiento.	Sistema operativo, aplicaciones, datos, accesos.
PaaS	Plataforma para desarrollar y ejecutar aplicaciones.	Aplicaciones, datos, permisos, configuración.
SaaS	Aplicación lista para usar.	Usuarios, datos, permisos, parámetros del servicio.

En IaaS, la organización tiene mayor control y mayor responsabilidad. En SaaS, el proveedor gestiona más componentes, pero la organización sigue siendo responsable de usuarios, permisos, datos cargados y configuración.

Ejemplo: si se usa un SaaS de gestión comercial, el proveedor mantiene la infraestructura. Pero si la organización otorga permisos de administrador a usuarios que no los necesitan, el riesgo es propio.

1.5.2 Nube pública, privada e híbrida

La nube pública es operada por un proveedor externo para múltiples clientes. La nube privada es dedicada a una organización. La nube híbrida combina infraestructura local con servicios en la nube. Cada modelo tiene implicancias distintas en control, costo, visibilidad y cumplimiento.

La nube híbrida es frecuente, pero compleja. Exige coherencia entre controles locales y controles en la nube: identidades, logs, cifrado, segmentación, monitoreo y procedimientos de recuperación.

1.5.3 Modelo de responsabilidad compartida

El modelo de responsabilidad compartida define qué gestiona el proveedor y qué gestiona el cliente. En términos generales, el proveedor es responsable de la seguridad de la nube; la organización es responsable de la seguridad en la nube.

Componente	Responsable típico
Centro de datos físico	Proveedor
Hardware e infraestructura base	Proveedor
Hipervisor y servicios administrados	Proveedor
Configuración de accesos	Organización
Datos cargados	Organización
Permisos de usuarios	Organización
Clasificación de información	Organización
Cumplimiento normativo del uso	Organización

Un bucket público por error, una base de datos expuesta o una cuenta con permisos excesivos suelen ser responsabilidad de la organización. No son fallas del proveedor si el servicio permite configurarlo de manera segura y fue configurado incorrectamente por el cliente.

1.5.4 Configuraciones inseguras

Las configuraciones inseguras son una causa frecuente de incidentes en la nube. Entre ellas se encuentran: almacenamiento público, permisos demasiado amplios, puertos abiertos a Internet, bases de datos sin cifrado, logs desactivados, claves de API sin rotación y cuentas administrativas sin MFA.

Configuración riesgosa	Impacto posible	Control
Bucket público accidental	Exposición de documentos.	Bloqueo de acceso público y revisión periódica.
Claves de API sin control	Acceso automatizado indebido.	Rotación, inventario y permisos mínimos.
Logs desactivados	Imposibilidad de investigar.	Activación y retención protegida.
Base de datos sin cifrado	Exposición de información sensible.	Cifrado en reposo y en tránsito.
Permisos excesivos	Escalamiento de privilegios.	Revisión periódica y RBAC.

1.5.5 Identidades y permisos

En la nube, las identidades no son solo usuarios humanos. También hay cuentas de servicio, funciones, máquinas virtuales, integraciones y claves programáticas. Cada identidad debe tener permisos mínimos y trazabilidad.

Los controles recomendables son MFA, roles por función, revisión de accesos, eliminación de claves no utilizadas, rotación de credenciales, privilegios temporales y monitoreo de actividad anómala.

1.5.6 Logs, CSPM y CASB

Los logs registran quién hizo qué, cuándo y desde dónde. Sin logs, la organización queda sin evidencia para investigar incidentes o demostrar cumplimiento.

El CSPM revisa continuamente configuraciones de nube y detecta desviaciones. Por ejemplo, puede alertar si un bucket se vuelve público o si una base de datos queda sin cifrado. El CASB controla el uso de servicios en la nube por parte de usuarios y ayuda a detectar aplicaciones no autorizadas.

1.5.7 Continuidad y dependencia del proveedor

La dependencia del proveedor puede convertirse en riesgo operativo. Si todos los procesos críticos dependen de un único proveedor y no existe plan de salida, una interrupción prolongada puede afectar ventas, nómina, documentos, correo y atención al cliente.

La administración debe evaluar:

- SLA del proveedor.
- Capacidad de exportar datos.
- Formatos estándar.
- Respaldos propios.
- Plan de salida.
- Pruebas de contingencia.
- Cláusulas contractuales de devolución y borrado de datos.

1.5.8 Ideas clave

- La nube redistribuye responsabilidades; no las elimina.
- En SaaS también existen responsabilidades del cliente.
- Las configuraciones inseguras son una fuente central de incidentes.
- Identidades, permisos, logs y cifrado deben gestionarse activamente.
- La dependencia del proveedor debe evaluarse como riesgo de continuidad.

1.6 Vulnerabilidades, bugs, exploits y gestión de parches

Una vulnerabilidad es una debilidad que puede ser aprovechada para afectar un activo. Puede estar en software, hardware, configuración, procesos, permisos, contraseñas, servicios expuestos o proveedores. Un bug es un error o defecto. No todo bug es

vulnerabilidad, pero algunos bugs pueden generar fallas de seguridad. Un exploit es el medio que permite aprovechar una vulnerabilidad.

La gestión de vulnerabilidades es preventiva y continua. No comienza cuando ocurre un incidente. Comienza con el inventario de activos, la identificación de debilidades, la priorización por riesgo, la aplicación de parches, el hardening, las excepciones formales y el seguimiento con indicadores.

1.6.1 Relación entre conceptos

Concepto	Definición simple	Ejemplo
Vulnerabilidad	Debilidad explotable.	Servidor sin parche crítico.
Amenaza	Actor o evento que puede aprovechar una debilidad.	Atacante externo o malware.
Bug	Error de software o lógica.	Cálculo incorrecto o validación incompleta.
Exploit	Técnica o código que aprovecha una vulnerabilidad.	Código que permite acceso no autorizado.
Riesgo	Combinación de probabilidad e impacto.	Sistema crítico expuesto con exploit público.

Desde administración, lo relevante no es aprender a explotar una falla, sino entender qué significa para el negocio. Una vulnerabilidad con exploit público en un sistema expuesto a Internet requiere atención urgente. Una vulnerabilidad similar en un laboratorio aislado puede tener menor prioridad.

1.6.2 CVE y CVSS

CVE identifica vulnerabilidades conocidas mediante un código único. Sirve para hablar del mismo problema sin confusión. CVSS asigna una puntuación de severidad, usualmente entre 0 y 10.

Sin embargo, CVSS no decide solo. La prioridad real depende del contexto: exposición a Internet, criticidad del activo, datos involucrados, existencia de exploit, controles compensatorios y capacidad de parcheo.

Criterio	Pregunta
Severidad técnica	¿Qué tan grave es la vulnerabilidad?
Exposición	¿El activo está accesible desde Internet?
Criticidad	¿Qué proceso depende del activo?
Datos	¿Hay información sensible?
Explotación activa	¿Se está usando en ataques reales?
Compensación	¿Existen controles que reduzcan el riesgo?

1.6.3 Inventario de activos

No se puede proteger lo que no se conoce. El inventario debe incluir sistemas, aplicaciones, servidores, estaciones, bases de datos, servicios en la nube, dominios, certificados, APIs, proveedores, responsables y criticidad.

Un escaneo puede detectar una vulnerabilidad crítica, pero si no se sabe qué proceso sostiene el servidor, quién es el dueño funcional o si está en producción, la corrección se demora. El inventario es una herramienta de gobierno.

1.6.4 Escaneo y pruebas de penetración

El escaneo de vulnerabilidades identifica debilidades conocidas de manera automatizada. La prueba de penetración valida si esas debilidades pueden explotarse en un contexto controlado. Son complementarias.

Actividad	Frecuencia esperada	Resultado
Escaneo de vulnerabilidades	Frecuente o continuo.	Lista de hallazgos para priorizar.
Prueba de penetración	Periódica o antes de cambios importantes.	Validación de riesgo real y recomendaciones.
Red team	Escenarios autorizados más amplios.	Evaluación de prevención, detección y respuesta.
Purple team	Colaboración ofensiva-defensiva.	Mejora concreta de controles.

El informe técnico debe transformarse en plan de acción: responsables, plazos, prioridades, excepciones y evidencia de cierre.

1.6.5 Patching y gestión de parches

Patching es la aplicación de actualizaciones para corregir vulnerabilidades o errores. Puede afectar sistemas operativos, aplicaciones, bases de datos, firmware, bibliotecas y servicios.

La aplicación de parches reduce riesgo, pero puede afectar continuidad si se hace sin pruebas. Por eso debe integrarse con gestión de cambios: evaluación, prueba, aprobación, ventana de mantenimiento, plan de reversión y verificación posterior.

Ejemplo de SLA de remediación:

Severidad	Plazo orientativo
Crítica con explotación activa	Urgente, según impacto.
Crítica en sistema expuesto	Hasta 7 días.
Alta en sistema crítico interno	Hasta 15 días.

Severidad	Plazo orientativo
Media	Hasta 30 días.
Baja	Hasta 90 días.

Estos plazos deben adaptarse a la organización. Si son imposibles, se incumplen siempre. Si son demasiado amplios, no reducen el riesgo.

1.6.6 Excepciones aceptadas por negocio

No siempre puede aplicarse un parche de inmediato. Puede haber incompatibilidades, sistemas heredados, dependencia de proveedor o riesgo operativo. En ese caso, la excepción debe ser formal.

Una excepción debe incluir activo, vulnerabilidad, riesgo, motivo, responsable del negocio, controles compensatorios, fecha de vencimiento, plan de remediación y aprobación. Una excepción sin vencimiento equivale a aceptar riesgo indefinidamente.

1.6.7 Hardening y baselines

Hardening significa endurecer la configuración: desactivar servicios innecesarios, cerrar puertos, restringir permisos, eliminar cuentas predeterminadas, activar logs, configurar cifrado y aplicar políticas seguras.

Una baseline es una configuración mínima esperada. Permite comparar el estado real contra el estado deseado. Los CIS Benchmarks pueden usarse como referencia para definir configuraciones seguras.

1.6.8 Ideas clave

- Vulnerabilidad, amenaza, exploit y riesgo no son lo mismo.
- CVSS orienta, pero el contexto del negocio decide la prioridad.
- El inventario de activos es base de la gestión de vulnerabilidades.
- Patching requiere equilibrio entre seguridad y continuidad.

- Las excepciones deben estar documentadas, justificadas y vencidas en el tiempo.

1.7 Ataques, malware y abuso de sistemas

Los ataques y el malware son riesgos centrales para organizaciones que dependen de sistemas de información. Pueden afectar datos, procesos, disponibilidad, reputación y obligaciones legales. Desde administración, no interesa solo la descripción técnica del ataque, sino qué proceso se afecta, qué evidencia queda, quién debe actuar y cómo se recupera la operación.

Un ataque es una acción deliberada para comprometer confidencialidad, integridad o disponibilidad. Un incidente es un evento que afecta o puede afectar la seguridad. El abuso de sistemas ocurre cuando una persona usa indebidamente un recurso al que puede tener acceso legítimo.

Ejemplo: un empleado autorizado para consultar clientes descarga toda la base para un uso no aprobado. No hubo malware ni intrusión externa, pero sí abuso de acceso.

1.7.1 Tipos de malware

Tipo	Característica	Riesgo administrativo
Virus	Se replica infectando archivos o programas.	Daño en documentos, planillas o carpetas compartidas.
Gusano	Se propaga por red con poca intervención del usuario.	Expansión rápida e interrupción.
Troyano	Parece legítimo, pero realiza acciones ocultas.	Robo de credenciales o instalación de acceso remoto.
Ransomware	Cifra o bloquea información.	Interrupción, pérdida de datos, extorsión.

Tipo	Característica	Riesgo administrativo
Spyware	Espía actividad del usuario.	Fuga de información sensible.
Keylogger	Registra pulsaciones de teclado.	Captura de contraseñas y datos bancarios.
Rootkit	Oculta presencia maliciosa.	Detección difícil y persistencia.
Backdoor	Permite acceso no autorizado posterior.	Reingreso del atacante aunque se cambien contraseñas.

La defensa requiere capas: actualización, protección de equipos finales, segmentación, backups protegidos, capacitación, monitoreo, gestión de privilegios y respuesta a incidentes.

1.7.2 Ataques sobre comunicaciones y red

Entre los ataques frecuentes se encuentran sniffing, spoofing, scanning, denegación de servicio, secuestro de sesión y movimiento lateral.

Ataque	Qué busca	Control relevante
Sniffing	Capturar tráfico.	Cifrado, TLS, segmentación.
Spoofing	Suplantar origen.	Autenticación, certificados, SPF/DKIM/DMARC.
Scanning	Identificar servicios o vulnerabilidades.	Monitoreo, cierre de puertos, firewall.

Ataque	Qué busca	Control relevante
DoS/DDoS	Interrumpir disponibilidad.	Mitigación, redundancia, monitoreo.
Hijacking de sesión	Usar una sesión válida robada.	TLS, cookies seguras, expiración, MFA.
Movimiento lateral	Desplazarse dentro de la red.	Segmentación, EDR, monitoreo interno.

No todo scanning produce daño inmediato, pero puede preparar un ataque posterior. Por eso, debe distinguirse entre escaneo autorizado y no autorizado.

1.7.3 Integridad, modificación y destrucción

Los ataques contra integridad son especialmente peligrosos porque el sistema puede seguir funcionando, pero con datos incorrectos. Pueden alterarse pagos, precios, descuentos, inventarios, reportes, archivos de importación o configuraciones.

Controles útiles:

- Segregación de funciones.
- Pistas de auditoría.
- Control de versiones.
- Hash y firma digital.
- Conciliaciones.
- Totales de control.
- Alertas por cambios sensibles.
- Revisión de accesos privilegiados.

Ejemplo: si se modifica una cuenta bancaria de proveedor sin autorización, el sistema puede procesar pagos correctamente desde el punto de vista técnico, pero hacia un destino fraudulento desde el punto de vista administrativo.

1.7.4 Backups como objetivo

Los respaldos son activos críticos. Un atacante puede intentar cifrarlos, borrarlos o modificarlos para impedir recuperación. Por eso, los backups deben protegerse con permisos restringidos, cifrado, retención, copias fuera del entorno principal, inmutabilidad y pruebas de restauración.

La regla 3-2-1 sirve como referencia: tres copias, en dos medios o ubicaciones, con una copia fuera del sitio principal o aislada. Para entornos críticos conviene agregar copias inmutables o desconectadas.

1.7.5 Ideas clave

- Malware y abuso interno pueden generar impactos similares sobre procesos.
- La integridad de datos es tan importante como la disponibilidad.
- Los respaldos deben protegerse como activos críticos.
- La segmentación limita la propagación y el movimiento lateral.
- La ausencia de alertas no garantiza ausencia de incidente.

1.8 Seguridad del correo electrónico y fraude organizacional

El correo electrónico es uno de los canales más usados en las organizaciones y uno de los vectores de ataque más frecuentes. Concentra facturas, instrucciones de pago, contratos, datos de clientes, datos de proveedores, comunicaciones de dirección y credenciales. Por eso, los atacantes lo utilizan para fraude, suplantación, robo de información y distribución de malware.

La seguridad del correo combina controles técnicos y administrativos. Los controles técnicos reducen mensajes maliciosos. Los controles administrativos evitan que una instrucción fraudulenta se convierta en una operación real.

1.8.1 Phishing, spear phishing y BEC

El phishing busca engañar al usuario para que entregue credenciales, abra archivos, ingrese a sitios falsos o ejecute acciones indebidas. El spear phishing es dirigido y personalizado. El BEC es el compromiso o abuso del correo empresarial para producir fraude.

Modalidad	Descripción	Ejemplo
Phishing	Mensaje masivo o general de engaño.	Correo falso de actualización de contraseña.
Spear phishing	Mensaje dirigido y personalizado.	Correo que menciona jefe, proveedor o proyecto real.
BEC	Fraude mediante correo empresarial.	Instrucción falsa de pago o cambio de cuenta bancaria.
CEO fraud	Suplantación de directivo.	Pedido urgente y confidencial de transferencia.
Vendor impersonation	Suplantación de proveedor.	Cambio falso de CBU.
Invoice fraud	Facturas falsas o manipuladas.	Factura de servicio inexistente.

El fraude suele apoyarse en urgencia, autoridad, confidencialidad y presión. Por eso, el control no puede depender solo de la atención del empleado.

1.8.2 SPF, DKIM y DMARC

SPF, DKIM y DMARC son estándares de autenticación de correo. Ayudan a reducir la suplantación de dominios.

Control	Función
SPF	Define qué servidores pueden enviar correos por un dominio.
DKIM	Firma mensajes para verificar integridad y origen del dominio.
DMARC	Define qué hacer si SPF o DKIM fallan y genera reportes.

Estos controles no eliminan todo riesgo. No impiden que un atacante use un dominio parecido ni que envíe correos desde una cuenta legítima comprometida. Por eso deben complementarse con capacitación, MFA, monitoreo y procedimientos de verificación.

1.8.3 Antispam, sandboxing y MFA

El antispam filtra mensajes sospechosos. El sandboxing ejecuta adjuntos en un entorno aislado para detectar comportamiento malicioso. MFA protege cuentas de correo ante robo de contraseña.

Una cuenta de correo comprometida es especialmente peligrosa porque el mensaje proviene de una dirección real. En ese caso, los controles de autenticación del dominio pueden no detectar el problema. Se requiere monitoreo de accesos, reglas de reenvío, inicios de sesión inusuales y actividad anómala.

1.8.4 Verificación fuera de banda

La verificación fuera de banda confirma una instrucción por un canal distinto al correo recibido. Es un control esencial contra BEC.

Ejemplo: si un proveedor solicita cambiar su CBU por correo, se debe llamar al número registrado previamente en el sistema, no al número incluido en el correo. Si el proveedor niega el cambio, se detecta el intento de fraude.

Este procedimiento debe ser obligatorio para:

- Cambios de cuentas bancarias.
- Pagos urgentes fuera del proceso habitual.
- Transferencias por encima de umbrales.
- Solicitudes de información sensible.
- Altas de proveedores.
- Modificaciones de datos críticos.

1.8.5 Doble aprobación y controles contables

La doble aprobación de pagos impide que una sola persona complete una operación riesgosa. También son útiles los umbrales por monto, la segregación de funciones, la auditoría de cambios en datos bancarios, la conciliación de pagos y las alertas por operaciones inusuales.

Ejemplo: un ERP puede bloquear pagos a proveedores cuyo CBU fue modificado en los últimos cinco días. Durante ese plazo, finanzas debe validar el cambio por canal independiente.

1.8.6 Ideas clave

- El correo electrónico combina riesgo técnico y riesgo administrativo.
- SPF, DKIM y DMARC reducen suplantación, pero no eliminan fraude.
- La verificación fuera de banda es clave para cambios de datos bancarios.
- La doble aprobación reduce el riesgo de transferencia fraudulenta.
- MFA y monitoreo son esenciales para cuentas de correo corporativo.

1.9 Seguridad de proveedores y cadena de suministro tecnológica

Ninguna organización opera sola. Contrata software, nube, soporte, desarrollo, consultoría, plataformas SaaS, servicios gestionados y componentes de código abierto. Cada relación con terceros introduce riesgo.

El riesgo de terceros es la exposición que surge por proveedores, socios, subcontratistas o componentes externos que tienen acceso a datos, sistemas o procesos de la organización. Contratar no elimina responsabilidad. Puede transferir parte del riesgo económico mediante cláusulas, pero la responsabilidad frente a clientes, empleados o reguladores puede seguir en la organización contratante.

1.9.1 Due diligence de proveedores

El due diligence es la evaluación previa a la contratación. Debe identificar riesgos antes de integrar al proveedor en procesos críticos.

Dimensión	Qué revisar
Certificaciones	ISO 27001, SOC 2, PCI DSS si corresponde.
Historial de incidentes	Brechas anteriores y mejoras implementadas.
Políticas de seguridad	Accesos, cifrado, incidentes, backups, subcontratistas.
Controles técnicos	MFA, logs, segmentación, vulnerabilidades, cifrado.
Ubicación de datos	Países, transferencias, cumplimiento legal.
Continuidad	Backups, recuperación, SLA, soporte.

El análisis debe ser proporcional. No se evalúa igual a un proveedor sin acceso a datos que a un proveedor de nómina o pagos.

1.9.2 Cláusulas contractuales de seguridad

El contrato debe establecer obligaciones de seguridad, notificación de incidentes, derecho de auditoría, confidencialidad, gestión de subcontratistas, devolución y borrado de datos, continuidad, SLA y penalidades.

Cláusula	Finalidad
Controles mínimos	Exigir prácticas de seguridad durante toda la relación.
Notificación de incidentes	Asegurar aviso oportuno ante eventos que afecten datos o sistemas.
Derecho de auditoría	Verificar cumplimiento.
Subcontratistas	Conocer y controlar cadena extendida.
Confidencialidad	Proteger información durante y después del contrato.
Offboarding	Revocar accesos, devolver datos y certificar borrado.

Un contrato sin derecho de auditoría deja a la organización dependiendo de declaraciones del proveedor.

1.9.3 SLA y criticidad

Los SLA definen compromisos cuantificados. No deben limitarse a disponibilidad. También pueden incluir tiempos de notificación de incidentes, tiempos de respuesta, frecuencia de pruebas de respaldo y tiempos de restauración.

Ejemplo: un SLA de 99,9% de disponibilidad permite hasta 8,76 horas de interrupción anual. Puede ser aceptable para un servicio secundario, pero insuficiente para pagos, nómina o ventas digitales.

1.9.4 Subcontratistas y cadena extendida

El proveedor principal puede usar subcontratistas. Si esos subcontratistas tienen acceso a datos o sistemas, la organización debe conocerlos y exigir que cumplan requisitos equivalentes. De lo contrario, puede aparecer un riesgo no visible.

1.9.5 SBOM y software de terceros

El SBOM es un inventario de componentes de software. Lista bibliotecas, versiones, dependencias y licencias. Permite saber rápidamente si una aplicación usa un componente vulnerable cuando se publica una nueva vulnerabilidad.

El uso de código abierto es normal y eficiente, pero requiere control de versiones, actualizaciones y monitoreo de vulnerabilidades.

1.9.6 Offboarding de proveedores

El offboarding es la salida segura del proveedor. Debe incluir revocación de accesos, devolución de datos, confirmación de borrado, eliminación de tokens, cierre de cuentas, recuperación de documentación y registro final.

Un proveedor que terminó contrato pero conserva accesos activos representa un riesgo innecesario.

1.9.7 Ideas clave

- El riesgo de terceros no se elimina al contratar.
- El due diligence debe realizarse antes de integrar al proveedor.
- Los contratos deben incluir obligaciones de seguridad y derecho de auditoría.
- La cadena de subcontratistas también debe ser visible.

- El offboarding es parte crítica del ciclo de vida del proveedor.

1.10 Gestión de incidentes de seguridad

Un incidente de seguridad es un evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de información, sistemas o servicios. Puede ser acceso no autorizado, malware, filtración, caída de sistemas, fraude digital, exposición accidental, pérdida de dispositivos, abuso de credenciales o compromiso de proveedor.

La gestión de incidentes no es solo una respuesta técnica. Incluye preparación, detección, análisis, contención, erradicación, recuperación, comunicación, evidencia, notificación, cierre y lecciones aprendidas.

1.10.1 Evento, alerta e incidente

Concepto	Descripción	Ejemplo
Evento	Ocurrencia observable.	Inicio de sesión de un usuario.
Alerta	Señal que requiere análisis.	Inicio de sesión desde ubicación inusual.
Incidente	Confirmación o sospecha fundada de compromiso.	Credenciales usadas por un tercero.

Distinguir estos niveles evita dos errores: tratar todo como crisis o ignorar señales relevantes.

1.10.2 Ciclo de respuesta

Fase	Objetivo	Ejemplo de acción
Preparación	Definir roles, planes, contactos y procedimientos.	Plan de respuesta y simulacros.

Fase	Objetivo	Ejemplo de acción
Identificación	Confirmar que existe un incidente.	Revisar logs y reportes.
Contención	Limitar daño y propagación.	Bloquear cuenta o aislar equipo.
Erradicación	Eliminar causa.	Quitar malware o corregir vulnerabilidad.
Recuperación	Restaurar servicios de forma segura.	Restaurar backup y validar integridad.
Lecciones aprendidas	Mejorar controles y procesos.	Informe final y acciones correctivas.

La recuperación debe hacerse con cuidado. Volver a encender un sistema comprometido sin validar puede reactivar el problema.

1.10.3 Severidad e impacto

La severidad indica gravedad y urgencia. El impacto mide consecuencias reales o potenciales. Deben considerarse sistemas críticos, datos sensibles, cantidad de afectados, exposición pública, duración, obligaciones legales, impacto financiero y continuidad.

Severidad	Criterio orientativo
Crítica	Afecta sistemas críticos, datos sensibles o continuidad significativa.
Alta	Impacto relevante pero controlable.
Media	Afectación limitada o contenida.

Severidad	Criterio orientativo
Baja	Evento menor, sin impacto material confirmado.

La severidad puede cambiar. Un caso inicialmente medio puede volverse crítico si se confirma exposición de datos o propagación activa.

1.10.4 Comunicación y notificación

La comunicación interna coordina acciones y reduce rumores. Debe ser clara, autorizada y ajustada al público. Los usuarios necesitan instrucciones operativas; los equipos técnicos necesitan detalles; la dirección necesita impacto y decisiones.

La comunicación externa puede involucrar clientes, proveedores, reguladores o prensa. Debe coordinarse con dirección, legales, seguridad y comunicación institucional. No deben emitirse afirmaciones no confirmadas.

Cuando corresponda notificar a clientes o reguladores, la organización debe tener criterios previos: plazos, responsables, contenido mínimo y evidencia.

1.10.5 Preservación de evidencia

La evidencia puede incluir logs, correos, capturas, archivos, imágenes de equipos, tickets, alertas, comunicaciones y línea de tiempo. Debe conservarse con trazabilidad: quién la obtuvo, cuándo, dónde se guardó y quién accedió.

Reiniciar un servidor puede ser necesario, pero también puede destruir evidencia volátil. Por eso, ante incidentes graves debe evaluarse qué preservar antes de modificar.

1.10.6 Línea de tiempo

La línea de tiempo ordena hechos, decisiones y acciones. Debe registrar inicio estimado, detección, primera alerta, activación del equipo, acciones de contención, comunicaciones, recuperación parcial, recuperación total y cierre.

Sin línea de tiempo, la organización depende de recuerdos. En una crisis, los recuerdos suelen ser incompletos.

1.10.7 Simulacros y ejercicios de mesa

Los simulacros permiten probar planes antes de un incidente real. Los tabletop exercises son ejercicios de discusión en los que se presenta un escenario y los participantes recorren decisiones, roles y comunicaciones.

Ejemplo de escenario: se detecta acceso no autorizado a una base de clientes. Hay indicios de descarga de datos. Un cliente pregunta en redes sociales si hubo filtración. El equipo debe decidir severidad, contención, comunicación, notificación y vocería.

1.10.8 Cierre del incidente

El cierre no debe ser solo técnico. Debe confirmar que el incidente fue contenido, la causa erradicada, los servicios recuperados, las comunicaciones realizadas, las evidencias preservadas y las acciones correctivas asignadas.

1.10.9 Ideas clave

- Todo incidente comienza con un evento, pero no todo evento es incidente.
- La preparación reduce improvisación.
- Contener no es lo mismo que erradicar.
- La comunicación debe basarse en hechos confirmados.
- Las lecciones aprendidas deben convertirse en acciones con responsables y plazos.

1.11 Relación entre los temas

Los temas vistos no son compartimentos aislados. Forman un sistema de gestión.

Tema	Se conecta con
Gobierno	Define responsables, políticas, indicadores y decisiones.
Comunicaciones	Protege datos en tránsito y validaciones entre sistemas.
Redes	Limita exposición, movimiento lateral y acceso indebido.
Nube	Requiere gestión de responsabilidades compartidas.
Vulnerabilidades	Reduce debilidades antes de que se conviertan en incidentes.
Malware y ataques	Explica amenazas que afectan activos y procesos.
Correo y fraude	Une seguridad técnica con control contable y financiero.
Proveedores	Extiende el riesgo más allá de la organización.
Incidentes	Integra preparación, respuesta, evidencia y recuperación.

Una organización con buen gobierno puede priorizar vulnerabilidades, exigir controles a proveedores, definir accesos mínimos, probar backups y responder mejor ante incidentes. Una organización sin gobierno puede tener muchas herramientas y, aun así, reaccionar tarde, comunicar mal o no conservar evidencia.

1.12 Ideas clave generales

- La seguridad de la información es una función de administración y gobierno.
- La protección debe centrarse en procesos, datos y activos críticos.
- La tecnología por sí sola no resuelve riesgos organizacionales.
- Los controles deben ser proporcionales al impacto y al contexto.
- La evidencia es indispensable para auditar, investigar y mejorar.
- Los proveedores, la nube y el correo amplían la superficie de riesgo.

- La continuidad del negocio depende de preparación, backups, recuperación y simulacros.
- La seguridad debe medirse con indicadores comprensibles para la dirección.
- Las excepciones deben estar documentadas, aprobadas y revisadas.
- La capacitación de usuarios debe integrarse con controles técnicos y procedimientos administrativos.

1.13 Preguntas de evaluación

1. ¿Por qué la seguridad de la información debe ser considerada una función de gobierno y no solo una tarea técnica?
2. Explique la diferencia entre confidencialidad, integridad y disponibilidad. Proponga un ejemplo administrativo para cada una.
3. ¿Qué función cumple una matriz RACI en la gestión de seguridad?
4. ¿Por qué una política de seguridad sin evidencia de cumplimiento tiene bajo valor administrativo?
5. Explique la diferencia entre evento, alerta e incidente.
6. ¿Qué información debería incluir una línea de tiempo de incidente?
7. ¿Por qué la aplicación de parches debe coordinarse con la gestión de cambios?
8. Explique la diferencia entre vulnerabilidad, amenaza, exploit y riesgo.
9. ¿Por qué CVSS no debe ser el único criterio de priorización de vulnerabilidades?
10. ¿Qué significa el modelo de responsabilidad compartida en la nube?
11. Indique tres configuraciones inseguras frecuentes en servicios de nube y su impacto.
12. ¿Por qué la segmentación de red reduce el impacto de un incidente?

13. Explique la función de una DMZ y proponga un ejemplo.
14. Compare firewall, IDS, IPS y WAF.
15. ¿Qué implica el enfoque Zero Trust?
16. ¿Por qué una VPN no garantiza por sí sola un acceso remoto seguro?
17. Explique la importancia de TLS, certificados digitales y firma digital en comunicaciones.
18. ¿Cuál es la diferencia entre un control de integridad técnico simple y una firma digital?
19. ¿Por qué el correo electrónico es un vector frecuente de fraude organizacional?
20. Explique cómo SPF, DKIM y DMARC contribuyen a reducir suplantaciones.
21. ¿Qué es la verificación fuera de banda y por qué es importante ante cambios de CBU?
22. ¿Qué controles contables pueden reducir el riesgo de fraude por correo electrónico?
23. ¿Por qué el riesgo de proveedores no desaparece al contratar un servicio externo?
24. ¿Qué debería incluir un due diligence de proveedores tecnológicos?
25. ¿Qué es un SBOM y qué utilidad tiene para la gestión de riesgo?
26. ¿Por qué el offboarding de proveedores debe ser un proceso formal?
27. ¿Qué riesgos genera un backup accesible desde la misma red comprometida?
28. ¿Por qué las lecciones aprendidas de un incidente deben convertirse en acciones concretas?
29. ¿Qué indicadores de seguridad serían relevantes para la alta gerencia?

30. Explique cómo se relacionan gobierno, vulnerabilidades, incidentes y continuidad del negocio.

1.14 Glosario de términos y siglas

Término o sigla	Explicación
API	Application Programming Interface. Interfaz de programación de aplicaciones que permite la comunicación entre sistemas.
BEC	Business Email Compromise. Compromiso o abuso del correo empresarial para cometer fraude.
BYOD	Bring Your Own Device. Uso de dispositivos personales para tareas laborales.
CASB	Cloud Access Security Broker. Intermediario de seguridad para controlar el acceso a servicios en la nube.
CIA	Confidentiality, Integrity, Availability. Confidencialidad, integridad y disponibilidad.
CISO	Chief Information Security Officer. Responsable principal de seguridad de la información.
CIS Benchmarks	Recomendaciones de configuración segura para distintas tecnologías.
Cloud computing	Computación en la nube. Uso de recursos tecnológicos contratados como servicio.
CRC	Cyclic Redundancy Check. Verificación por redundancia cíclica para detectar errores accidentales.

Término o sigla	Explicación
CSPM	Cloud Security Posture Management. Gestión de postura de seguridad en la nube.
CVE	Common Vulnerabilities and Exposures. Identificador público de vulnerabilidades conocidas.
CVSS	Common Vulnerability Scoring System. Sistema de puntuación de severidad de vulnerabilidades.
DKIM	DomainKeys Identified Mail. Firma de correo basada en claves de dominio.
DMARC	Domain-based Message Authentication, Reporting and Conformance. Política de autenticación y reporte de correo.
DMZ	Demilitarized Zone. Zona desmilitarizada; segmento intermedio entre Internet y la red interna.
DNS	Domain Name System. Sistema de nombres de dominio que traduce nombres en direcciones IP.
DNSSEC	Domain Name System Security Extensions. Extensiones de seguridad para DNS.
DLP	Data Loss Prevention. Prevención de pérdida de datos.
DoS	Denial of Service. Denegación de servicio.
DDoS	Distributed Denial of Service. Denegación de servicio distribuida.
EDR	Endpoint Detection and Response. Detección y respuesta en equipos finales.

Término o sigla	Explicación
ERP	Enterprise Resource Planning. Sistema de planificación de recursos empresariales.
Exploit	Técnica, código o procedimiento que aprovecha una vulnerabilidad.
Firewall	Cortafuegos. Control que filtra tráfico entre redes o sistemas.
Hardening	Endurecimiento de configuración para reducir superficie de ataque.
Hash	Huella digital calculada sobre datos para detectar cambios.
HMAC	Hash-Based Message Authentication Code. Código de autenticación de mensaje basado en hash y clave.
HTTPS	HTTP Secure. Protocolo web protegido mediante TLS.
IaaS	Infrastructure as a Service. Infraestructura como servicio.
IAM	Identity and Access Management. Gestión de identidades y accesos.
IDS	Intrusion Detection System. Sistema de detección de intrusiones.
IoT	Internet of Things. Internet de las cosas; dispositivos conectados.
IPS	Intrusion Prevention System. Sistema de prevención de intrusiones.
Keylogger	Software o dispositivo que registra pulsaciones del teclado.
KPI	Key Performance Indicator. Indicador clave de desempeño.

Término o sigla	Explicación
MFA	Multi-Factor Authentication. Autenticación multifactor.
mTLS	Mutual TLS. TLS mutuo; autenticación de cliente y servidor mediante certificados.
NAC	Network Access Control. Control de acceso a la red.
NDR	Network Detection and Response. Detección y respuesta en red.
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework. Marco de ciberseguridad del NIST.
Open source	Código abierto. Software cuyo código fuente puede ser usado, revisado o modificado según licencia.
PaaS	Platform as a Service. Plataforma como servicio.
PCI DSS	Payment Card Industry Data Security Standard. Estándar de seguridad para datos de tarjetas de pago.
Phishing	Técnica de engaño para obtener credenciales, datos o acciones de la víctima.
PKI	Public Key Infrastructure. Infraestructura de clave pública para certificados y firmas.
RACI	Responsible, Accountable, Consulted, Informed. Matriz de responsabilidades.
Ransomware	Malware que cifra o bloquea información y exige una condición para recuperarla.

Término o sigla	Explicación
RBAC	Role-Based Access Control. Control de acceso basado en roles.
RPO	Recovery Point Objective. Objetivo de punto de recuperación; pérdida máxima de datos aceptable.
RTO	Recovery Time Objective. Objetivo de tiempo de recuperación; tiempo máximo tolerable de interrupción.
SaaS	Software as a Service. Software como servicio.
Sandbox	Entorno aislado para ejecutar archivos o procesos sin afectar sistemas reales.
SBOM	Software Bill of Materials. Inventario de componentes de software.
SIEM	Security Information and Event Management. Gestión de información y eventos de seguridad.
SLA	Service Level Agreement. Acuerdo de nivel de servicio.
SOC 2	Service Organization Control 2. Informe de controles de una organización de servicios.
SPF	Sender Policy Framework. Registro que indica qué servidores pueden enviar correo por un dominio.
SQL	Structured Query Language. Lenguaje de consulta estructurada usado en bases de datos.
SSO	Single Sign-On. Inicio de sesión único.

Término o sigla	Explicación
TLS	Transport Layer Security. Protocolo de seguridad para comunicaciones cifradas.
Typosquatting	Registro de nombres similares a dominios legítimos para engañar usuarios.
VLAN	Virtual Local Area Network. Red local virtual para segmentar redes.
VPN	Virtual Private Network. Red privada virtual para crear un canal protegido.
WAF	Web Application Firewall. Firewall de aplicaciones web.
WPA2 / WPA3	Wi-Fi Protected Access. Estándares de seguridad para redes inalámbricas.
XDR	Extended Detection and Response. Detección y respuesta extendida.
Zero Trust	Modelo de confianza cero: ningún acceso se considera confiable por defecto.
ZTNA	Zero Trust Network Access. Acceso a red basado en confianza cero.