Paper elaborado por Aníbal M. Mazza Fraquelli Doctor de la Universidad de Buenos Aires, en base a la desgrabación de sus clases. Se permite la reproducción total o parcial CITANDO LA FUENTE.
Actualizado a: **30 de mayo de 2026**

Amenazas a los sistemas de información desde la administración de Tecnologías de la Información

1.1 Presentación del tema

Los sistemas de información son componentes centrales de la operación organizacional. Registran ventas, compras, cobranzas, pagos, inventarios, sueldos, contratos, clientes, proveedores, comunicaciones, reportes y decisiones. Cuando esos sistemas fallan, se interrumpen o son manipulados, la organización puede sufrir pérdidas económicas, errores operativos, incumplimientos legales, exposición de datos y deterioro de su capacidad de gestión.

Una amenaza es cualquier evento, condición o conducta con capacidad de afectar la confidencialidad, integridad o disponibilidad de la información. La confidencialidad busca impedir accesos no autorizados. La integridad exige que los datos sean correctos y no sean alterados indebidamente. La disponibilidad requiere que la información y los servicios estén accesibles cuando se necesitan. Estas tres dimensiones integran la triada CIA, por sus siglas en inglés: *Confidentiality, Integrity and Availability*.

Desde la administración de Tecnologías de la Información, las amenazas no deben analizarse solo como ataques externos. También incluyen errores de usuarios, fallas de hardware, problemas eléctricos, incendios, cambios no controlados en programas, accesos indebidos, robo de datos, fraude financiero, abuso de privilegios, sabotaje, fallas de proveedores y desastres.

Para estudiantes de administración de empresas, el punto central consiste en comprender que una amenaza tecnológica casi siempre tiene consecuencias organizacionales. Un servidor caído puede impedir facturar. Un dato alterado puede producir pagos incorrectos. Una cuenta con privilegios excesivos puede facilitar fraude. Una copia de respaldo inexistente puede transformar una falla menor en una interrupción grave.

La identificación de amenazas es, por lo tanto, una tarea de gestión. Requiere vincular tecnología, procesos, personas, activos, controles, costos e impacto sobre el negocio.

1.2 Amenazas, impactos y controles

Una amenaza debe analizarse en relación con el activo afectado, la vulnerabilidad existente, el impacto posible y el control aplicable. No alcanza con nombrar el problema. Es necesario comprender qué consecuencia puede producir en la organización y qué medidas permiten reducir el riesgo.

Elemento de análisis	Pregunta administrativa	Ejemplo
Activo afectado	¿Qué información, sistema o proceso puede verse comprometido?	Sistema de facturación
Amenaza	¿Qué evento puede causar daño?	Corte eléctrico
Vulnerabilidad	¿Qué debilidad permite que el daño ocurra o se agrave?	Falta de energía de respaldo
Impacto	¿Qué consecuencia tendrá sobre el negocio?	Imposibilidad de emitir facturas
Control	¿Qué medida reduce la probabilidad o el impacto?	UPS, generador, plan de continuidad
Evidencia	¿Cómo se demuestra que el control existe y funciona?	Pruebas, reportes, registros y auditorías

Este enfoque permite convertir una amenaza técnica en un problema administrable. La organización puede priorizar, asignar responsables, presupuestar controles y verificar resultados.

1.3 Amenazas físicas e infraestructura

Las amenazas físicas afectan instalaciones, equipos, cableado, soportes de almacenamiento y condiciones ambientales. Incluyen incendios, inundaciones, humedad,

temperatura inadecuada, polvo, cortes edilicios, acceso físico no autorizado, robo de equipos, daño accidental y desastres naturales.

La protección física es parte de la seguridad de la información. No debe tratarse como un tema exclusivamente edilicio. Un servidor protegido lógicamente puede quedar comprometido si cualquier persona accede a la sala donde se encuentra. Una notebook sin cifrado puede exponer datos sensibles si se pierde o es robada. Un disco externo con copias de respaldo puede convertirse en una fuente de filtración si no está protegido.

Amenaza física	Consecuencia posible	Control recomendado
Incendio	Pérdida de equipos, documentos y soportes	Detectores, extintores adecuados y plan de emergencia
Inundación	Daño a servidores o cableado	Ubicación segura de equipos y monitoreo ambiental
Robo de notebook	Exposición de información	Cifrado de disco, inventario y bloqueo remoto
Acceso físico no autorizado	Manipulación de equipos o extracción de datos	Tarjetas de acceso, cerraduras y registro de visitantes
Temperatura inadecuada	Daño o caída de equipos críticos	Climatización, sensores y mantenimiento preventivo

Desde administración, estas amenazas exigen políticas de acceso físico, inventario de activos, procedimientos de retiro de equipos, responsables de custodia y controles periódicos.

1.4 Problemas eléctricos y servicios básicos

Los sistemas de información dependen de energía eléctrica, climatización, conectividad y servicios de soporte. Un corte eléctrico puede detener servidores, redes, puestos de trabajo, sistemas de atención y comunicaciones. Una variación de tensión puede dañar hardware. Una falla de climatización puede afectar equipos críticos por exceso de temperatura.

La administración debe distinguir qué servicios son críticos y cuánto tiempo pueden permanecer interrumpidos. No todos los sistemas tienen la misma urgencia. Un sistema de facturación, una plataforma de ventas o un sistema de pagos suelen requerir mayor prioridad que aplicaciones auxiliares.

Servicio básico	Riesgo asociado	Control posible
Energía eléctrica	Caída de servidores y puestos de trabajo	UPS, generadores y apagado ordenado
Climatización	Sobrecalentamiento de equipos	Sensores, alarmas y mantenimiento
Conectividad	Interrupción de operaciones en línea	Enlaces redundantes y proveedores alternativos
Cableado	Fallas de red o cortes internos	Canalización, identificación y mantenimiento
Servicios de soporte	Demoras en recuperación	Contratos con tiempos de respuesta definidos

Ejemplo: si el sistema de facturación tiene un RTO de cuatro horas, la infraestructura eléctrica debe permitir sostenerlo o recuperarlo dentro de ese plazo. Si no existe energía de respaldo, ese objetivo no es realista.

1.5 Fallas de hardware

El hardware comprende los componentes físicos de procesamiento, almacenamiento y comunicación. Pueden fallar discos, memorias, fuentes, placas, servidores, routers, switches, notebooks, impresoras y dispositivos de almacenamiento.

La falla de hardware no siempre produce pérdida de datos, pero puede generar interrupciones significativas. Si un disco falla y no existen arreglos redundantes, copias de respaldo o equipos de reemplazo, la recuperación puede demorar. Si falla un equipo de comunicaciones en una sucursal, esa sede puede quedar sin acceso al sistema central.

Componente	Falla posible	Impacto administrativo
Servidor	Interrupción del servicio	Paralización de sistemas críticos
Disco	Pérdida o inaccesibilidad de datos	Recuperación desde backups
Router o switch	Corte de conectividad	Sucursal o sector sin acceso
Notebook	Pérdida de equipo o información	Exposición de datos y reemplazo operativo
Impresora crítica	Interrupción documental	Demoras en procesos administrativos

La gestión debe incluir inventario, mantenimiento, garantías, repuestos críticos, monitoreo, renovación planificada y respaldos. También debe diferenciar equipos comunes de componentes críticos. Un teclado defectuoso no tiene el mismo impacto que un servidor de base de datos sin redundancia.

1.6 Fallas de software y cambios en programas

El software puede fallar por errores de programación, actualizaciones defectuosas, incompatibilidades, configuraciones incorrectas o cambios no probados. Un cambio en un programa puede alterar cálculos, permisos, reportes, integraciones o reglas de negocio.

En administración, los cambios en sistemas deben gestionarse formalmente. La gestión de cambios permite reducir el riesgo de introducir errores en ambientes productivos.

Etapa de gestión de cambios	Finalidad
Solicitud	Registrar qué cambio se necesita y por qué
Análisis de impacto	Evaluar procesos, datos, usuarios y sistemas afectados
Prueba	Verificar que el cambio funcione antes de implementarlo
Aprobación	Confirmar que el área responsable acepta el cambio
Implementación	Aplicar el cambio en condiciones controladas
Plan de reversión	Definir cómo volver atrás si el cambio falla
Registro final	Documentar fecha, responsable y resultado

Ejemplo: una modificación en el sistema de descuentos comerciales puede generar facturas con importes incorrectos. Si no se prueba antes de aplicar el cambio, el error puede afectar cientos de operaciones. Un control adecuado es probar casos representativos, aprobar el cambio por el área responsable y revisar los resultados luego de implementarlo.

1.7 Acciones del personal y errores de usuarios

Las personas pueden cometer errores, omitir procedimientos, compartir contraseñas, enviar información al destinatario equivocado, cargar datos incorrectos, borrar archivos,

aprobar operaciones sin revisar o instalar aplicaciones no autorizadas. Muchas veces no existe intención de causar daño, pero el impacto puede ser alto.

Un error de usuario puede afectar la integridad o la disponibilidad de la información. Cargar mal una cuenta bancaria de proveedor puede producir un pago incorrecto. Borrar una carpeta compartida puede interrumpir un proceso. Enviar un archivo con datos personales a un destinatario equivocado puede generar exposición de información.

Error de usuario	Dimensión afectada	Control preventivo
Carga incorrecta de datos	Integridad	Validaciones, doble revisión y reglas de negocio
Borrado accidental	Disponibilidad	Permisos limitados, backups y papelera controlada
Envío a destinatario equivocado	Confidencialidad	Clasificación, advertencias y capacitación
Aprobación sin revisión	Integridad	Circuitos de aprobación y evidencia obligatoria
Instalación no autorizada	Integridad y disponibilidad	Bloqueo de instalaciones y software permitido

La prevención requiere capacitación, controles de validación, doble revisión en operaciones críticas, perfiles adecuados, restricciones de eliminación, confirmaciones antes de acciones irreversibles y registros de actividad. También se necesita una cultura que favorezca el reporte temprano de errores. Ocultar un error suele aumentar el daño.

1.8 Accesos no permitidos y abuso de privilegios

El acceso no permitido se produce cuando una persona ingresa a un sistema, dato o recurso sin autorización. Puede ocurrir mediante credenciales robadas, contraseñas

compartidas, cuentas activas de personas desvinculadas, permisos mal asignados o fallas de configuración.

El abuso de privilegios aparece cuando alguien tiene acceso autorizado, pero lo usa para fines indebidos o fuera de su función. Este riesgo es especialmente importante en sistemas administrativos, contables, de pagos, compras, sueldos y gestión de proveedores.

Situación	Riesgo	Control recomendado
Cuenta de persona desvinculada sigue activa	Acceso indebido	Baja inmediata y revisión de usuarios
Permisos excesivos	Fraude o error	Principio de mínimo privilegio
Cuenta administrativa compartida	Falta de trazabilidad	Cuentas individuales y registros de actividad
Usuario aprueba sus propias operaciones	Conflicto de funciones	Separación de funciones
Acceso externo sin control	Ingreso no autorizado	MFA, VPN y monitoreo

El principio de mínimo privilegio indica que cada usuario debe contar solo con los permisos requeridos para su tarea. Las cuentas administrativas deben ser limitadas, monitoreadas y revisadas con mayor frecuencia.

1.9 Robo de datos y fuga de información

El robo de datos puede producirse por copia no autorizada, extracción mediante credenciales, acceso de terceros, malware, pérdida de dispositivos o abuso interno. La fuga de información puede ser intencional o accidental.

La información comprometida puede incluir bases de clientes, listados de precios, diseños, contratos, legajos, credenciales, documentación contable, reportes financieros o datos de proveedores. El impacto puede ser económico, legal, competitivo y reputacional.

Tipo de información	Impacto posible
Base de clientes	Reclamos, sanciones y pérdida de confianza
Listas de precios	Daño competitivo
Legajos de personal	Conflictos legales y exposición de datos personales
Contratos	Incumplimiento de confidencialidad
Credenciales	Nuevos accesos indebidos
Reportes financieros	Daño reputacional o uso indebido

Los controles incluyen clasificación de información, cifrado, monitoreo de descargas, restricciones de exportación, control de dispositivos externos, registros de acceso, acuerdos de confidencialidad y revisión de permisos. En entornos con mayor exposición, puede aplicarse DLP, es decir, prevención de pérdida de datos.

1.10 Código malicioso: virus, gusanos, troyanos y ransomware

El código malicioso es software diseñado para causar daño, obtener acceso indebido o utilizar recursos de manera no autorizada. Incluye virus, gusanos, troyanos, ransomware, spyware y otras variantes.

Tipo de código malicioso	Característica principal	Impacto posible
Virus	Se adhiere a archivos o programas y se propaga al ejecutarse	Alteración o daño de archivos
Gusano	Se replica por redes con baja intervención del usuario	Saturación, propagación e interrupciones

Tipo de código malicioso	Característica principal	Impacto posible
Troyano	Aparenta ser legítimo, pero ejecuta acciones ocultas	Robo de credenciales o acceso remoto
Ransomware	Cifra o bloquea información	Interrupción operativa y extorsión
Spyware	Espía actividad o captura información	Pérdida de confidencialidad

Estas amenazas pueden afectar disponibilidad, integridad y confidencialidad. Pueden cifrar servidores, borrar datos, capturar contraseñas, abrir accesos remotos, alterar archivos o enviar información al exterior.

Los controles básicos incluyen actualización de sistemas, protección de equipos finales, filtrado de correo, restricción de ejecución de archivos, copias de respaldo, segmentación de red, monitoreo de eventos y capacitación sobre correos engañosos. Un backup no probado no garantiza recuperación. La restauración debe verificarse periódicamente.

1.11 Atacantes informáticos y accesos externos

El término hacker suele usarse de manera amplia para referirse a personas con habilidades técnicas que exploran o manipulan sistemas. En seguridad organizacional conviene diferenciar entre investigación autorizada, acceso no autorizado y ataque. El problema para la organización aparece cuando un actor externo intenta ingresar, alterar, interrumpir, robar o defraudar mediante sistemas.

Los accesos externos pueden incluir fuerza bruta contra contraseñas, explotación de vulnerabilidades, engaños por correo, ataques a servicios publicados, denegación de servicio o ataques distribuidos.

Tipo de ataque externo	Descripción	Control posible
Fuerza bruta	Prueba masiva de contraseñas	Bloqueo por intentos fallidos y MFA
Explotación de vulnerabilidad	Uso de una falla técnica conocida	Actualización y gestión de vulnerabilidades
Phishing	Engaño para obtener datos o credenciales	Capacitación, filtros y reportes tempranos
DoS	Interrupción deliberada de disponibilidad	Protección de red y monitoreo
DDoS	Ataque distribuido desde múltiples fuentes	Servicios de mitigación y arquitectura resiliente

La organización debe reducir exposición. Esto implica mantener sistemas actualizados, aplicar autenticación multifactor, limitar servicios publicados, monitorear intentos fallidos, revisar configuraciones, gestionar vulnerabilidades y definir procedimientos de respuesta ante incidentes.

1.12 Amenazas vinculadas con clientes, proveedores, socios y aliados

Los terceros pueden ser fuente de riesgo. Clientes, proveedores, vendedores, socios comerciales y aliados pueden interactuar con sistemas, plataformas, extranets, portales o integraciones. Esa interacción puede ser necesaria para el negocio, pero aumenta la superficie de exposición.

Un proveedor con acceso remoto puede convertirse en vía de ingreso si usa contraseñas débiles. Un cliente puede cargar información falsa o aprovechar una falla de validación. Un socio comercial puede recibir información que no corresponde a su función. Un servicio externo puede fallar y afectar operaciones internas.

Tercero	Riesgo posible	Control recomendado
Proveedor de soporte	Acceso remoto indebido	MFA, contrato, registro de actividad y baja oportuna
Cliente	Carga de datos falsos o uso indebido del portal	Validaciones y monitoreo
Socio comercial	Acceso a información no necesaria	Perfiles limitados y confidencialidad
Servicio externo	Interrupción de operaciones internas	Acuerdos de nivel de servicio y plan alternativo
Consultor temporal	Conservación de accesos vencidos	Fecha de expiración y revisión periódica

La gestión de terceros debe incluir contratos, perfiles de acceso, confidencialidad, autenticación, registros de actividad, revisión periódica de permisos, evaluación de seguridad y procedimiento de baja. Ningún tercero debería conservar accesos indefinidos sin necesidad vigente.

1.13 Fraude financiero mediante sistemas

El fraude financiero mediante sistemas puede adoptar distintas formas: modificación de cuentas bancarias, generación de pagos indebidos, alteración de facturas, creación de proveedores ficticios, manipulación de descuentos, cambios en condiciones comerciales o uso de credenciales ajenas para aprobar operaciones.

Estos fraudes suelen combinar debilidades técnicas y administrativas. Un sistema puede permitir modificar datos sin aprobación. Un usuario puede tener permisos excesivos. Un proceso puede carecer de revisión independiente. Una alerta puede no existir o no ser revisada.

Riesgo de fraude	Debilidad frecuente	Control recomendado
Cambio de cuenta bancaria de proveedor	Falta de doble aprobación	Validación documental y confirmación por canal independiente
Proveedor ficticio	Alta sin revisión	Control de altas y revisión periódica
Pago indebido	Permisos acumulados	Separación de funciones y límites por monto
Descuento comercial manipulado	Reglas sin control	Aprobación por responsable y auditoría
Aprobación con credenciales ajenas	Contraseñas compartidas	MFA, trazabilidad y sanciones internas

Ejemplo: todo cambio de cuenta bancaria de proveedor debería requerir documentación, aprobación de un responsable distinto y confirmación por un canal independiente. Esta práctica reduce el riesgo de fraude y mejora la evidencia disponible.

1.14 Robo de software y uso no autorizado de programas

El robo de software puede comprender copia, instalación, distribución o uso no autorizado de programas. También puede incluir uso de licencias fuera de los términos permitidos. Desde administración, esta amenaza genera riesgos legales, económicos, técnicos y de seguridad.

El software no autorizado puede contener malware, carecer de actualizaciones o provocar incompatibilidades. Además, dificulta inventariar activos y controlar soporte. Una organización que permite instalaciones libres pierde visibilidad sobre su entorno tecnológico.

Riesgo	Consecuencia	Control
Uso de software sin licencia	Reclamos legales o sanciones	Gestión de licencias
Instalación de programas no autorizados	Malware o incompatibilidad	Bloqueo de instalaciones
Falta de inventario	Desconocimiento del entorno	Relevamiento periódico
Software obsoleto	Vulnerabilidades sin corregir	Actualización y retiro planificado
Repositorios no confiables	Descarga de código dañino	Repositorios aprobados

El área de TI debe saber qué software existe, quién lo usa, con qué licencia y para qué proceso. Esta información permite reducir riesgos y ordenar costos.

1.15 Sabotaje y daño deliberado

El sabotaje implica una acción intencional destinada a dañar, interrumpir o degradar sistemas, datos o servicios. Puede provenir de personal interno, terceros con acceso, competidores desleales o atacantes externos. Puede manifestarse como borrado de datos, eliminación de respaldos, alteración de configuraciones, interrupción de servicios o introducción de código dañino.

El riesgo aumenta cuando existen privilegios excesivos, falta de monitoreo, ausencia de segregación de funciones, cuentas compartidas o demoras en revocar accesos.

Señal de riesgo	Control necesario
Accesos de personas desvinculadas	Baja inmediata y verificación
Usuarios con privilegios excesivos	Revisión periódica y mínimo privilegio

Señal de riesgo	Control necesario
Eliminación de logs	Registros protegidos e inalterables
Borrado de backups	Copias protegidas e inmutables
Cambios fuera de horario sin autorización	Alertas y revisión de actividades anómalas

Los controles incluyen baja inmediata de usuarios, control de cuentas privilegiadas, registros protegidos, backups resguardados, revisión de cambios, monitoreo de actividades anómalas y planes de recuperación. También deben existir procedimientos para preservar evidencia si se sospecha una conducta deliberada.

1.16 Desastres y continuidad operativa

Los desastres pueden ser naturales, técnicos, humanos u organizacionales. Incluyen incendios, inundaciones, cortes prolongados, indisponibilidad de proveedores críticos, fallas masivas, incidentes de seguridad graves y pérdida de instalaciones. Su característica principal es que superan el incidente ordinario y afectan la continuidad del negocio.

La continuidad operativa requiere identificar procesos esenciales, definir tiempos de recuperación, establecer puntos máximos de pérdida de información, documentar procedimientos alternativos y probarlos.

Concepto	Pregunta que responde	Ejemplo
Proceso crítico	¿Qué actividad debe sostenerse o recuperarse primero?	Facturación, pagos, atención al cliente
RTO	¿Cuánto tiempo puede estar caído el servicio?	El sistema debe volver en seis horas

Concepto	Pregunta que responde	Ejemplo
RPO	¿Cuánta información puede perderse medida en tiempo?	Se acepta perder como máximo dos horas de datos
Procedimiento alternativo	¿Cómo se opera durante la interrupción?	Registro manual temporal o sistema alternativo
Prueba de continuidad	¿El plan funciona en la práctica?	Simulacro o prueba documentada

Ejemplo: si la organización acepta perder como máximo dos horas de datos, los respaldos diarios son insuficientes. Si el servicio debe volver en seis horas, no alcanza con tener equipos de reemplazo disponibles recién a los tres días.

1.17 Matriz sintética de amenazas y controles

La siguiente matriz resume las principales amenazas, sus impactos administrativos y controles orientativos.

Amenaza	Impacto administrativo	Controles principales
Incendio o inundación	Pérdida de equipos, documentos y continuidad	Protección física, backups externos y plan de emergencia
Corte eléctrico	Interrupción de sistemas críticos	UPS, generadores y procedimientos de apagado
Falla de hardware	Caída de servicios o pérdida de acceso	Inventario, mantenimiento, redundancia y repuestos
Cambio de software defectuoso	Errores en operaciones o reportes	Gestión de cambios, pruebas y plan de reversión

Amenaza	Impacto administrativo	Controles principales
Error de usuario	Datos incorrectos o pérdida de información	Capacitación, validaciones y revisión
Acceso no permitido	Exposición o manipulación de datos	MFA, mínimo privilegio y monitoreo
Abuso de privilegios	Fraude o uso indebido	Segregación de funciones y auditoría
Robo de datos	Daño legal, económico y reputacional	Cifrado, DLP, clasificación y registros
Malware	Interrupción, robo o alteración	Actualizaciones, protección de endpoints y backups
Riesgo de terceros	Exposición por proveedores o socios	Contratos, perfiles, MFA y revisión de accesos
Fraude financiero	Pérdida patrimonial	Doble aprobación, límites y conciliación
Software no autorizado	Riesgo legal y técnico	Inventario, licencias y bloqueo de instalaciones
Sabotaje	Daño deliberado o interrupción	Baja inmediata, monitoreo y registros protegidos
Desastre	Interrupción grave del negocio	Plan de continuidad, RTO, RPO y pruebas

1.18 Ideas clave

- Las amenazas a los sistemas de información no se limitan a ataques externos.

- Una amenaza técnica puede convertirse rápidamente en un problema administrativo y económico.
- La triada CIA permite analizar si se afecta confidencialidad, integridad o disponibilidad.
- Las amenazas físicas también forman parte de la seguridad de la información.
- Los problemas eléctricos, de conectividad y climatización pueden afectar la continuidad operativa.
- Las fallas de hardware y software requieren inventario, mantenimiento, pruebas y gestión de cambios.
- Los errores de usuarios deben tratarse con capacitación, validaciones y controles de proceso.
- El abuso de privilegios puede ser tan riesgoso como un acceso externo no autorizado.
- La fuga de información puede ser intencional o accidental.
- El malware puede afectar datos, sistemas, credenciales y operaciones completas.
- Los proveedores, clientes y socios amplían la superficie de exposición.
- El fraude financiero suele combinar debilidades técnicas y administrativas.
- Los planes de continuidad deben definir RTO, RPO y procedimientos alternativos.
- La seguridad eficaz depende de controles técnicos, administrativos y humanos coordinados.

1.19 Conclusión

Las amenazas a los sistemas de información son diversas y no se limitan a ataques externos. Incluyen fallas de hardware, errores de software, problemas eléctricos,

incendios, errores de usuarios, accesos indebidos, abuso de privilegios, robo de datos, código malicioso, fallas de comunicaciones, riesgos de terceros, fraude financiero, robo de software, sabotaje y desastres.

Desde la administración, cada amenaza debe vincularse con activos, procesos e impactos. La pregunta no es solo qué puede ocurrir, sino qué operación se afectaría, cuánto tiempo podría detenerse, qué datos podrían perderse, qué controles existen y qué evidencia permitiría responder.

Una amenaza técnica puede convertirse en un problema de negocio. Un cambio mal probado puede generar facturación incorrecta. Una baja de usuario demorada puede permitir acceso indebido. Un proveedor sin controles puede abrir una vía de exposición. Un backup no probado puede impedir recuperar información crítica.

Para estudiantes de administración de empresas, la enseñanza central consiste en comprender que la seguridad de los sistemas de información requiere clasificación, prevención, controles y revisión continua. La organización debe identificar amenazas internas y externas, reducir vulnerabilidades, preparar respuestas, auditar controles y capacitar a las personas.

La seguridad eficaz no depende de una medida aislada. Depende de un conjunto ordenado de decisiones administrativas y técnicas.

1.20 Preguntas de evaluación

1. ¿Qué es una amenaza a los sistemas de información?
2. ¿Por qué las amenazas no deben limitarse a ataques externos?
3. ¿Cómo se relacionan las amenazas con la confidencialidad, integridad y disponibilidad?
4. ¿Por qué las amenazas físicas forman parte de la seguridad de la información?
5. ¿Cómo pueden los problemas eléctricos afectar la continuidad operativa?

6. ¿Qué controles reducen el impacto de fallas de hardware?
7. ¿Por qué la gestión de cambios es importante frente a fallas de software?
8. ¿Cómo pueden los errores de usuarios afectar la integridad de la información?
9. ¿Qué diferencia existe entre acceso no permitido y abuso de privilegios?
10. ¿Qué riesgos genera el robo de datos para una organización?
11. ¿Cuál es la diferencia entre virus, gusano, troyano, ransomware y spyware?
12. ¿Por qué proveedores, clientes y socios comerciales pueden representar amenazas?
13. ¿Qué controles ayudan a prevenir fraude financiero mediante sistemas?
14. ¿Por qué el uso de software no autorizado genera riesgos legales y técnicos?
15. ¿Qué condiciones aumentan el riesgo de sabotaje?
16. ¿Por qué los planes de continuidad deben definir RTO y RPO?
17. ¿Qué evidencia debería conservarse frente a un incidente de seguridad?
18. ¿Cómo puede una amenaza técnica transformarse en un problema de negocio?

1.21 Glosario de términos y siglas

Término o sigla	Explicación
Amenaza (*threat*)	Evento, condición o conducta con capacidad de causar daño a datos, sistemas o procesos.
Availability	Disponibilidad. Propiedad que exige que la información y los sistemas estén accesibles cuando se necesitan.

Término o sigla	Explicación
Backup	Copia de respaldo destinada a recuperar información ante pérdida, daño o interrupción.
Change management	Gestión de cambios. Proceso formal para solicitar, evaluar, aprobar, probar e implementar cambios en sistemas.
CIA (*Confidentiality, Integrity and Availability*)	Triada de la seguridad de la información: confidencialidad, integridad y disponibilidad.
Cifrado (*encryption*)	Técnica que transforma información para impedir su lectura por personas no autorizadas.
Confidentiality	Confidencialidad. Propiedad que limita el acceso a la información solo a personas autorizadas.
DDoS (*Distributed Denial of Service*)	Ataque distribuido de denegación de servicio, realizado desde múltiples fuentes para afectar la disponibilidad.
DLP (*Data Loss Prevention*)	Prevención de pérdida de datos. Conjunto de herramientas y controles para evitar salidas no autorizadas de información.
DoS (*Denial of Service*)	Denegación de servicio. Ataque destinado a impedir o degradar el acceso a un sistema o servicio.

Término o sigla	Explicación
Endpoint	Equipo final utilizado por usuarios, como notebook, computadora de escritorio, celular o tablet.
Encryption	Cifrado. Protección de información mediante técnicas criptográficas.
Hardware	Componentes físicos de procesamiento, almacenamiento y comunicación.
Integrity	Integridad. Propiedad que exige que los datos sean correctos, completos y no alterados indebidamente.
Least privilege	Principio de mínimo privilegio. Cada usuario debe tener solo los permisos necesarios para cumplir su función.
Malware (*malicious software*)	Software malicioso diseñado para causar daño, obtener acceso indebido o usar recursos sin autorización.
MFA (*Multi-Factor Authentication*)	Autenticación multifactor. Método que exige más de un factor para validar el acceso.
Ransomware	Tipo de malware que cifra o bloquea información y exige una condición o pago para recuperarla.

Término o sigla	Explicación
RPO (*Recovery Point Objective*)	Objetivo de punto de recuperación. Indica cuánta información puede perderse medida en tiempo.
RTO (*Recovery Time Objective*)	Objetivo de tiempo de recuperación. Indica cuánto tiempo puede estar caído un servicio.
Segregation of duties	Separación de funciones. Distribución de tareas incompatibles entre distintas personas para reducir errores o fraudes.
Software	Programas, aplicaciones, sistemas operativos y componentes lógicos utilizados por la organización.
Spyware	Software malicioso destinado a espiar actividad o capturar información.
Threat	Amenaza. Evento o condición con capacidad de causar daño.
Trojan horse	Caballo de Troya. Programa que aparenta ser legítimo, pero ejecuta acciones ocultas.
UPS (*Uninterruptible Power Supply*)	Sistema de alimentación ininterrumpida que permite sostener equipos ante cortes o variaciones eléctricas.

Término o sigla	Explicación
VPN (*Virtual Private Network*)	Red privada virtual usada para crear una conexión segura hacia recursos internos desde redes externas.
Worm	Gusano. Malware que puede replicarse por redes y propagarse rápidamente.