Gestión de Riesgos en Tecnologías de la Información

1.1 Introducción

La gestión de riesgos en TI no es un asunto exclusivo del área técnica. Las organizaciones dependen de datos, aplicaciones, redes, proveedores y plataformas digitales para operar. Cada decisión tecnológica lleva implícita una exposición al riesgo que la administración debe conocer, evaluar y gestionar.

Un error en la carga de datos, una caída del sistema de facturación, una filtración de información personal, la pérdida de respaldos o un acceso no autorizado pueden afectar ventas, costos, reputación, obligaciones legales y continuidad operativa. Por eso, el riesgo tecnológico debe analizarse como parte de la gestión general de la organización: con los mismos criterios con que se analizan los riesgos financieros, operativos o legales.

La gestión de riesgos en profundidad parte de una idea central: no alcanza con identificar una amenaza aislada o instalar un control puntual. Un riesgo tecnológico no surge de un único elemento. Aparece cuando un activo valioso está expuesto, presenta debilidades, enfrenta amenazas y se encuentra dentro de un contexto organizacional, humano, técnico, económico y regulatorio determinado.

1.2 La información como activo crítico de la organización

La información no es solamente un conjunto de archivos, planillas, correos electrónicos o registros administrativos. En una organización, la información es un **activo crítico** porque permite operar, controlar, decidir, cumplir obligaciones y sostener la continuidad del negocio.

Una empresa puede tener edificios, maquinarias, dinero, mercadería y personal. Sin embargo, si pierde la información que permite saber qué vendió, a quién debe cobrar, a quién debe pagar, qué contratos firmó, qué empleados tiene, qué impuestos debe presentar o qué stock posee, su capacidad de funcionamiento queda seriamente afectada.

Desde la administración, considerar la información como un activo implica reconocer que debe ser protegida, clasificada, controlada, respaldada y auditada. No se trata solo de "guardar datos": se trata de asegurar que esos datos puedan ser utilizados correctamente por las personas autorizadas, en el momento necesario y con el nivel de confianza adecuado.

Tipo de información	Ejemplo	Riesgo principal
Contable	Mayores, balances, asientos, reportes financieros	Alteración o pérdida de integridad
Comercial	Clientes, precios, descuentos, condiciones de venta	Uso indebido o fuga de datos
De proveedores	CUIT, CBU, contratos, órdenes de compra	Fraude o modificación no autorizada
Laboral	Legajos, sueldos, sanciones, evaluaciones	Acceso no autorizado
Operativa	Pedidos, stock, entregas, reclamos	Interrupción o datos incompletos
Estratégica	Planes, presupuestos, negociaciones	Espionaje o pérdida de confidencialidad

Cuando se comprende que la información tiene valor económico y organizacional, resulta más sencillo justificar controles de seguridad, capacitación, auditorías, políticas de acceso, procedimientos de respaldo y planes de continuidad.

1.3 La organización como sistema expuesto al riesgo

Una organización puede entenderse como un sistema compuesto por personas, procesos, tecnología, datos, proveedores, contratos, controles, normas y decisiones. El riesgo

aparece cuando cualquiera de esos elementos puede fallar, ser vulnerado, actuar de manera indebida o quedar fuera de control.

Los riesgos organizacionales vinculados con TI no se limitan a virus, ataques informáticos o fallas de servidores. También incluyen errores humanos, autorizaciones mal definidas, falta de capacitación, proveedores sin control, procesos sin documentación, baja tardía de usuarios, cambios no aprobados, ausencia de respaldo, incumplimiento normativo y decisiones gerenciales tomadas sin información suficiente.

Elemento de la organización	Pregunta de riesgo
Personas	¿Tienen los accesos adecuados? ¿Saben cómo actuar ante incidentes?
Procesos	¿Existen controles, autorizaciones y evidencias?
Sistemas	¿Están protegidos, actualizados y monitoreados?
Datos	¿Están clasificados, respaldados y protegidos?
Proveedores	¿Cumplen requisitos de seguridad y confidencialidad?
Dirección	¿Define prioridades, recursos y apetito de riesgo?
Auditoría	¿Verifica que los controles funcionen?

La gestión de riesgos en TI requiere una mirada interdisciplinaria: tecnología implementa controles, pero administración define prioridades, recursos, responsabilidades, procedimientos y criterios de aceptación.

1.4 La tríada CIA: confidencialidad, integridad y disponibilidad

La seguridad de la información se apoya en tres principios fundamentales conocidos como **tríada CIA**. Estos principios permiten clasificar los efectos principales de un riesgo sobre la información.

Principio	Significado	Ejemplo organizacional	Pregunta de control
Confidencialidad	La información solo debe ser accesible para personas autorizadas	Un empleado sin permisos accede a legajos salariales	¿Quién puede ver esta información?
Integridad	La información debe mantenerse completa, exacta y sin alteraciones indebidas	Se modifica el CBU de un proveedor sin validación	¿Cómo se garantiza que el dato no fue alterado?
Disponibilidad	Los sistemas y datos deben estar accesibles cuando se necesitan	El sistema de facturación cae durante el horario comercial	¿Cuánto tiempo puede estar caído este sistema?

Un mismo evento puede afectar más de un principio. Por ejemplo, un ransomware puede afectar la **disponibilidad** porque impide acceder a los archivos; también puede afectar la **confidencialidad** si el atacante copió información antes de cifrarla; y puede afectar la **integridad** si los archivos fueron modificados o dañados.

1.5 Componentes del riesgo

El riesgo se materializa cuando una **amenaza** aprovecha una **vulnerabilidad** para afectar un **activo de información**. Comprender cada componente por separado permite construir análisis más precisos y diseñar controles más eficaces.

Componente	Definición	Ejemplo en TI
Activo	Elemento con valor para la organización que requiere protección	Base de datos de clientes, ERP, credenciales, procesos
Exposición	Condición que acerca el activo al daño	Servidor publicado en Internet sin segmentación
Vulnerabilidad	Debilidad que puede ser explotada por una amenaza	Contraseña débil, ausencia de MFA, sistema sin parches
Amenaza	Evento o condición capaz de causar daño	Ransomware, phishing, error humano, falla de proveedor
Impacto	Consecuencia de la materialización del riesgo	Pérdida de datos, interrupción, sanciones, daño reputacional
Probabilidad	Posibilidad de que el evento ocurra en un período determinado	Alta, media, baja según frecuencia histórica y controles existentes

La **combinación de probabilidad e impacto** determina el nivel de riesgo y, por tanto, la urgencia de la respuesta.

1.5.1 El activo

Un activo puede ser **digital**, **físico**, de **conocimiento**, **intangible**, **humano** o vinculado a un **método o proceso**. No todos los activos tienen la misma criticidad: una impresora de oficina y la base de datos del sistema de pagos no deben gestionarse con el mismo nivel de protección.

Tipo de activo	Ejemplo en TI
Datos	Base de clientes, legajos de personal, registros contables
Sistemas	ERP, CRM, sistema de nómina
Infraestructura	Servidores, red, routers, firewalls, dispositivos móviles
Aplicaciones	Portal web, sistema de tickets, aplicación de ventas
Credenciales	Contraseñas, tokens, certificados digitales
Procesos	Circuito de aprobación de pagos, alta y baja de usuarios
Personas	Administradores, usuarios clave, técnicos especializados
Conocimiento	Configuraciones críticas, manuales, lógica de negocio

1.5.2 La exposición

La exposición es la condición que acerca el activo al daño. Un activo puede existir y ser valioso, pero su nivel de riesgo cambiará según su grado de exposición. La exposición no es todavía una vulnerabilidad; es una condición de accesibilidad o cercanía al riesgo que indica dónde profundizar el análisis.

Activo	Forma de exposición
Base de datos de clientes	Accesible desde Internet sin segmentación adecuada
Credenciales de servicio	Guardadas en un archivo visible para varios usuarios
Sistema web	Publicado con formularios abiertos al exterior
Notebook corporativa	Utilizada fuera de la oficina en redes públicas
Repositorio documental	Compartido con permisos excesivos
Aplicación en nube	Expuesta por mala configuración de accesos

1.5.3 La vulnerabilidad

La vulnerabilidad es la debilidad que puede ser explotada. Puede estar en la tecnología, en el proceso o en las personas.

Tipo	Ejemplo en TI
Técnica	Sistema sin parches, software obsoleto, mala configuración
Humana	Usuario que comparte contraseñas o cae en phishing
Procesal	No existe revisión periódica de permisos
Contractual	Proveedor accede sin controles definidos
Documental	No hay inventario actualizado de activos

Tipo	Ejemplo en TI
Organizacional	Roles y responsabilidades de seguridad no definidos

Ejemplo: si el activo es un sistema de nómina y el acceso se realiza por Internet a través de VPN, la vulnerabilidad puede consistir en que la autenticación depende solo de una contraseña, sin MFA. Allí aparece una debilidad concreta que una amenaza podría aprovechar.

1.5.4 La amenaza

La amenaza es el agente, acción o evento capaz de explotar una vulnerabilidad y causar daño. No siempre es un atacante externo: también puede incluir errores humanos, abuso interno, fallas de terceros o incidentes físicos.

Tipo de amenaza	Ejemplo
Malware / Ransomware	Software que cifra datos y exige rescate
Phishing	Correo falso que roba credenciales
Abuso interno	Empleado con permisos válidos que extrae datos
Proveedor comprometido	Tercero que ingresa con acceso remoto y causa daño
Error humano	Carga errónea o envío indebido de información
Interrupción física	Corte eléctrico en sala de servidores
Exposición en nube	Recurso configurado como público por error

Una amenaza no genera necesariamente daño por sí sola: para que el riesgo se materialice, debe encontrar un activo expuesto y una vulnerabilidad explotable.

1.6 Fuentes de riesgo en el manejo de la información

Los riesgos pueden provenir de cuatro grandes categorías.

1.6.1 Personal interno

El personal posee acceso legítimo a sistemas, datos y procesos. Por error, descuido, desconocimiento, negligencia o intención maliciosa, una persona con acceso autorizado puede generar daño.

Riesgo interno	Descripción	Ejemplo
Error humano	Equivocación sin intención de dañar	Enviar una base de clientes al destinatario equivocado
Abuso de acceso	Uso de permisos más allá de la función asignada	Consultar sueldos sin autorización funcional
Fraude	Manipulación de datos para obtener un beneficio indebido	Modificar datos bancarios de un proveedor
Sabotaje	Daño intencional a sistemas o información	Eliminar archivos antes de una desvinculación
Uso indebido de herramientas	Utilización de aplicaciones no aprobadas	Subir contratos a una cuenta personal en la nube

Los controles aplicables incluyen segregación de funciones, revisión de permisos, capacitación, monitoreo, políticas de uso aceptable, procedimientos de alta y baja de usuarios, y auditoría de cambios sensibles.

1.6.2 Terceros

Los terceros pueden ser proveedores, consultores, socios comerciales, auditores o prestadores de servicios. En muchos casos, tienen acceso a datos o sistemas de la organización.

Actor externo	Riesgo posible	Ejemplo
Proveedor tecnológico	Acceso excesivo o credenciales activas innecesarias	Conserva acceso luego de finalizar el contrato
Consultor externo	Uso inadecuado de información interna	Descarga documentación confidencial sin autorización
Socio comercial	Exposición por integración de sistemas	Una API mal configurada comparte datos de más
Atacante externo	Acceso no autorizado o robo de datos	Obtiene credenciales mediante phishing

La gestión de terceros exige contratos, acuerdos de confidencialidad, revisión de accesos, cláusulas de seguridad y procedimientos de finalización de la relación.

1.6.3 Ambiente físico

El riesgo físico también afecta la seguridad de la información. Un servidor sin protección física, una sala técnica sin control de acceso o una notebook sin cifrado pueden generar incidentes tan graves como un ataque digital.

Riesgo físico	Impacto posible	Control recomendado
Incendio	Pérdida de equipos y documentación	Detección y supresión de incendios

Riesgo físico	Impacto posible	Control recomendado
Inundación	Daño a servidores o dispositivos	Ubicación segura de infraestructura crítica
Corte eléctrico	Interrupción de sistemas	UPS y generador, según criticidad
Robo de equipos	Pérdida de información y credenciales	Cifrado de disco y bloqueo remoto
Sala técnica sin control	Manipulación indebida de infraestructura	Cerraduras, cámaras y registro de ingresos

El ambiente físico y el ambiente digital deben analizarse en conjunto.

1.6.4 Eventos tecnológicos

Evento	Descripción	Impacto posible
Malware	Software diseñado para dañar, espiar o controlar sistemas	Robo de datos, interrupción o pérdida de información
Ransomware	Malware que cifra datos y exige pago	Paralización de operaciones y extorsión
Phishing	Engaño para obtener credenciales o información	Acceso indebido a sistemas
Troyano	Programa que aparenta ser legítimo	Robo de credenciales o instalación de malware adicional
Gusano	Malware que se propaga por redes	Saturación de red e infección masiva

La prevención requiere controles combinados: capacitación, filtros de correo, MFA, actualización de sistemas, EDR, backups, segmentación de red, monitoreo y respuesta ante incidentes.

1.7 El proceso formal de gestión del riesgo

La gestión formal del riesgo es un **ciclo continuo** de seis pasos. No es un evento puntual.

Paso	Acción	Qué debe producirse
1	Identificar activos	Inventario con nombre, responsable, función, criticidad, usuarios y dependencias
2	Identificar amenazas y vulnerabilidades	Lista de eventos posibles para cada activo y debilidades que los habilitan
3	Valorar probabilidad e impacto	Justificación de cada valor asignado (no solo el número)
4	Definir el tratamiento	Decisión documentada con responsable, fecha y recursos asignados
5	Implementar controles	Controles verificables: frecuencia, responsable, retención y prueba de restauración
6	Monitorear y revisar	Revisión periódica: trimestral en sistemas críticos, semestral o anual en sistemas menos sensibles

La formalidad es importante porque permite comparar riesgos, justificar inversiones, asignar responsables, documentar decisiones y demostrar diligencia ante auditorías, autoridades, clientes o tribunales.

Un plan sin responsable definido suele convertirse en una intención sin ejecución. Un backup no probado no garantiza recuperación.

1.8 Identificación de riesgos

Identificar riesgos significa responder de manera ordenada a la pregunta: **¿qué puede salir mal?** La identificación debe considerar riesgos visibles y no visibles: dependencias críticas, proveedores, procesos manuales, errores frecuentes, sistemas sin dueño, usuarios con privilegios elevados, respaldos no probados y cumplimiento normativo.

Técnica	Utilidad
Entrevistas con responsables de proceso	Detectar riesgos operativos no visibles para TI
Talleres de riesgo	Reunir áreas para analizar escenarios
Revisión de incidentes históricos	Aprender de eventos anteriores
Auditorías y revisiones de control	Detectar debilidades documentales o técnicas
Escaneos técnicos	Identificar vulnerabilidades de sistemas
Análisis de proveedores	Evaluar riesgos derivados de terceros
Revisión normativa	Identificar obligaciones legales y contractuales

Un riesgo identificado pero no documentado queda sujeto a la memoria de las personas y pierde valor como herramienta de gestión.

1.9 Análisis cualitativo y cuantitativo

1.9.1 Análisis cualitativo

El análisis cualitativo clasifica los riesgos mediante categorías (baja, media, alta, crítica). Es más simple y rápido; resulta útil cuando no existen datos históricos suficientes o cuando se necesita una primera priorización.

Categoría	Probabilidad	Impacto
Baja	Es poco probable que ocurra	Consecuencia menor
Media	Puede ocurrir en determinadas condiciones	Consecuencia moderada
Alta	Es probable que ocurra	Consecuencia importante
Crítica	Es muy probable o ya ocurrió	Consecuencia severa

Su principal limitación es la subjetividad. Dos personas pueden valorar de manera diferente el mismo riesgo si no existen criterios claros y compartidos.

1.9.2 Análisis cuantitativo

El análisis cuantitativo intenta expresar el riesgo en valores numéricos, generalmente económicos. Requiere estimar probabilidad e impacto monetario.

Pérdida esperada = Probabilidad del evento × Impacto económico estimado

Concepto	Valor
Probabilidad anual de ransomware	15%
Impacto económico estimado	USD 300.000
Pérdida esperada anual	**USD 45.000**

Este cálculo permite comparar el costo de los controles con la pérdida que se busca reducir. Sin embargo, no todos los impactos pueden medirse con precisión: la reputación, la confianza de clientes o el daño institucional suelen requerir estimaciones prudentes.

1.10 Probabilidad e impacto — Matriz y mapa de calor

1.10.1 Escala de valoración

Valor	Probabilidad	Criterio orientativo	Impacto	Criterio orientativo en TI
1	Muy baja	Puede ocurrir en casos excepcionales	Muy bajo	Interrupción menor, sin pérdida de datos ni efecto operativo relevante
2	Baja	Podría ocurrir, pero no es frecuente	Bajo	Afecta a pocos usuarios o requiere corrección simple
3	Media	Puede ocurrir algunas veces al año	Medio	Afecta un proceso interno, genera demoras o reprocesos

Valor	Probabilidad	Criterio orientativo	Impacto	Criterio orientativo en TI
4	Alta	Es probable si no hay controles	Alto	Afecta clientes, facturación, cumplimiento o datos sensibles
5	Muy alta	Se espera que ocurra con frecuencia	Muy alto	Interrumpe procesos críticos, genera pérdida de datos, sanciones o daño reputacional

Nivel de riesgo = Probabilidad × Impacto

1.10.2 Mapa de calor

Probabilidad / Impacto	1 Muy bajo	2 Bajo	3 Medio	4 Alto	5 Muy alto
5 Muy alta	5 Medio	10 Alto	15 Alto	20 **Crítico**	25 **Crítico**
4 Alta	4 Bajo	8 Medio	12 Alto	16 Alto	20 **Crítico**
3 Media	3 Bajo	6 Medio	9 Medio	12 Alto	15 Alto
2 Baja	2 Bajo	4 Bajo	6 Medio	8 Medio	10 Alto
1 Muy baja	1 Bajo	2 Bajo	3 Bajo	4 Bajo	5 Medio

1.10.3 Regla de tratamiento según nivel

Nivel	Clasificación	Acción sugerida
1 a 5	Bajo	Aceptar con monitoreo básico
6 a 9	Medio	Mitigar con controles razonables y seguimiento periódico
10 a 16	Alto	Mitigar con prioridad; transferir parcialmente si corresponde; reportar a la dirección
17 a 25	**Crítico**	Evitar, rediseñar el proceso, suspender la actividad o implementar controles inmediatos

1.10.4 Ejemplo de matriz aplicada

Riesgo	Prob.	Impacto	Nivel	Tratamiento sugerido
Phishing a usuarios administrativos	4	4	16 Alto	Capacitación, MFA, filtros de correo y simulacros
Ransomware en servidor de archivos	4	5	20 Crítico	Backups probados, EDR

Riesgo	Prob.	Impacto	Nivel	Tratamiento sugerido y plan de continuidad
Baja tardía de exempleados	3	5	15 Alto	Baja automática y revisión de accesos
Error en datos bancarios de proveedor	4	4	16 Alto	Doble aprobación y auditoría de cambios
Pérdida de notebook sin cifrado	2	5	10 Alto	Cifrado, bloqueo remoto y reporte obligatorio
Corte eléctrico breve	3	3	9 Medio	UPS y monitoreo de energía
Caída de sitio institucional fuera de horario	2	2	4 Bajo	Monitoreo básico y soporte

La matriz no debe usarse como un trámite formal. Debe servir para decidir prioridades, asignar recursos y exigir responsables.

1.11 Riesgo inherente, residual y aceptado

Concepto	Explicación	Ejemplo
Riesgo inherente	Riesgo existente antes de aplicar controles	Base de datos expuesta a Internet sin protección
Riesgo residual	Riesgo que permanece después de aplicar controles	Base protegida con MFA, firewall y monitoreo, pero aún vulnerable a ataques sofisticados
Riesgo aceptado	Parte del riesgo residual que la organización decide asumir formalmente	La dirección acepta el riesgo documentadamente porque está dentro del apetito definido

La seguridad absoluta no existe. Todo control reduce el riesgo, pero no lo elimina por completo. Por eso, la administración debe decidir qué nivel residual puede aceptar.

Aceptar un riesgo no significa ignorarlo. Significa reconocerlo, documentarlo, justificar la decisión, asignar un responsable y establecer una fecha de revisión.

1.12 Apetito y tolerancia al riesgo

El **apetito de riesgo** indica cuánto riesgo está dispuesta a asumir una organización para alcanzar sus objetivos. Es una decisión de gobierno que debe traducirse en criterios operativos concretos, no en declaraciones genéricas.

La **tolerancia al riesgo** indica el margen de variación aceptable alrededor de ese apetito.

Concepto	Pregunta	Ejemplo
Apetito de riesgo	¿Cuánto riesgo se acepta en condiciones normales?	No aceptar accesos a sistemas críticos sin MFA

Concepto	Pregunta	Ejemplo
Tolerancia al riesgo	¿Qué margen excepcional se admite?	Admitir una demora máxima de 6 horas ante una falla crítica excepcional

Ejemplos de criterios operativos del apetito de riesgo: - La organización acepta interrupciones menores a 30 minutos en sistemas internos no críticos. - No acepta más de 5 minutos de caída en la plataforma de ventas durante el horario comercial. - Acepta errores administrativos menores corregibles, pero no acepta accesos no autorizados a datos personales.

Sin criterios definidos, la gestión del riesgo se reduce a reacciones ante incidentes, no a decisiones anticipadas.

1.13 Estrategias de tratamiento del riesgo

Una vez evaluado el riesgo, la organización debe decidir qué hacer. Las cuatro estrategias no son equivalentes: cada una aplica según la naturaleza del riesgo, el proceso afectado, el costo del control y la tolerancia organizacional.

Estrategia	En qué consiste	Cuándo aplicarla
Evitar	No iniciar, discontinuar o modificar una actividad para eliminar la exposición	Cuando el riesgo supera el apetito y la actividad no es indispensable
Mitigar / reducir	Implementar controles para reducir probabilidad, impacto o ambos	Cuando el sistema no puede dejar de usarse pero puede protegerse mejor
Transferir / compartir	Trasladar total o parcialmente el impacto a un tercero	Cuando parte del riesgo puede cubrirse con contratos, SLA o seguros

Estrategia	En qué consiste	Cuándo aplicarla
Aceptar / asumir	Reconocer el riesgo formalmente sin implementar controles adicionales	Cuando el riesgo está dentro del apetito o el costo de mitigarlo supera el beneficio

1.13.1 Evitar el riesgo

Evitar no significa actuar con temor: significa reconocer que ciertas exposiciones no se justifican. Se aplica cuando: - No se implementa una aplicación gratuita que exige cargar datos sensibles en servidores sin garantías adecuadas. - No se habilitan accesos administrativos desde redes públicas. - No se almacenan datos que no son necesarios para el proceso. Si un dato no se recolecta, no puede filtrarse.

1.13.2 Mitigar el riesgo

Es la estrategia más frecuente en TI. La mitigación no elimina el riesgo: lo reduce a un nivel aceptable. Por eso es necesario medir el riesgo antes y después del control.

Ejemplo: un sistema de pagos con doble aprobación para transferencias superiores a un umbral definido. El control reduce la probabilidad de fraude interno o error operativo. Los registros de auditoría permiten verificar quién inició la operación, quién la aprobó y cuándo.

1.13.3 Transferir el riesgo

Transferir el riesgo **no elimina la responsabilidad de la organización**: distribuye consecuencias mediante contratos, seguros o acuerdos. La organización sigue siendo responsable de evaluar si los niveles pactados son suficientes.

Lo que debe incluir un contrato con un proveedor:

Elemento	Por qué es necesario
Niveles de servicio (SLA)	Define compromisos medibles de disponibilidad y tiempos de respuesta
Confidencialidad	Protege la información compartida con el tercero
Ubicación de los datos	Determina qué legislación aplica y qué garantías existen
Subcontrataciones	Permite conocer qué terceros adicionales intervienen
Notificación de incidentes	Establece plazos y canales para informar fallas de seguridad
Derecho de auditoría	Permite verificar el cumplimiento contractual
Devolución o eliminación de datos al finalizar	Protege la información cuando termina la relación

Un seguro no reemplaza los controles. Si la organización no cuenta con backups, políticas de acceso o registros adecuados, el seguro puede no cubrir determinados eventos.

1.13.4 Aceptar el riesgo

Aceptar un riesgo no es ignorarlo. La aceptación debe quedar **documentada** e incluir: quién la aprueba, qué riesgo se acepta, la justificación de la decisión, el período durante el cual se mantiene, y la fecha de revisión. Una aceptación sin fecha de revisión puede convertirse en una debilidad permanente.

1.14 Controles de seguridad

Los controles son las medidas que la organización implementa para reducir riesgos. Pueden ser técnicos, administrativos, físicos, manuales o automáticos.

Tipo de control	Objetivo	Ejemplo
Preventivo	Evitar que el incidente ocurra	MFA, cifrado, segregación de funciones, actualizaciones, capacitación
Disuasivo	Desalentar antes de que ocurra	Políticas visibles, monitoreo conocido, advertencias
Detectivo	Descubrir que algo ocurrió o está ocurriendo	Logs, alertas, auditorías, SIEM
Correctivo	Corregir o contener el problema detectado	Bloqueo de cuenta, reversión de cambio, cierre de vulnerabilidad
Recuperatorio	Restaurar la operación después del incidente	Backups, plan de continuidad, sitio alternativo

Un programa de control efectivo combina varios tipos. Frente al riesgo de phishing, por ejemplo:

Control	Tipo	Efecto esperado
Capacitación sobre phishing	Preventivo	Reducir la probabilidad de engaño
MFA	Preventivo	Impedir que una contraseña robada sea suficiente
Filtro antiphishing	Preventivo / detectivo	Bloquear o marcar correos sospechosos

Control	Tipo	Efecto esperado
Monitoreo de accesos	Detectivo	Identificar accesos desde ubicaciones inusuales
Procedimiento de respuesta	Correctivo	Bloquear la cuenta y revisar acciones realizadas
Backups y continuidad	Recuperatorio	Recuperar operación si el ataque escala

La selección de controles debe relacionarse con los riesgos identificados. **No conviene aplicar controles costosos a riesgos bajos, ni dejar sin control riesgos altos.** La eficiencia requiere proporcionalidad.

1.15 Defensa en profundidad

La defensa en profundidad consiste en aplicar **capas de control**. La organización no debe depender de una única barrera: si un control falla, otro debe reducir el impacto.

Capa	Control
1	Capacitación del usuario
2	Política de contraseñas
3	MFA
4	Control de acceso basado en roles
5	Monitoreo de logs
6	Segmentación de red
7	Backups probados
8	Plan de respuesta ante incidentes

Capa	Control
9	Plan de continuidad
10	Auditoría y mejora continua

Esta lógica permite comprender por qué no alcanza con comprar una herramienta aislada. La seguridad se construye con controles combinados, personas capacitadas, procedimientos claros y revisión permanente.

1.16 Registro de riesgos y dueño del riesgo

El **registro de riesgos** es el documento o sistema donde se consolida la información relevante de cada riesgo identificado. Permite seguimiento, control y rendición de cuentas.

Campo del registro	Contenido esperado
ID	Código único del riesgo
Descripción	Evento de riesgo redactado con claridad
Activo o proceso afectado	Sistema, dato o circuito comprometido
Causa probable	Amenaza o vulnerabilidad asociada
Probabilidad	Valor estimado y justificación
Impacto	Valor estimado y justificación
Nivel de riesgo inherente	Riesgo antes de controles
Controles existentes	Medidas actuales
Riesgo residual	Riesgo luego de controles
Tratamiento definido	Evitar, mitigar, transferir o aceptar
Dueño del riesgo	Responsable de gestionarlo

Campo del registro	Contenido esperado
Fecha de revisión	Momento de actualización

El **dueño del riesgo** no siempre es el responsable técnico. Si el riesgo afecta el proceso de liquidación de sueldos, el dueño puede ser Recursos Humanos, aunque TI implemente parte de los controles. Si el riesgo afecta pagos a proveedores, el dueño puede ser Finanzas o Administración.

En gestión, un riesgo sin dueño es un riesgo sin gobierno.

1.17 Indicadores de riesgo y de gestión

Sin indicadores, la organización trabaja con percepciones. Los indicadores permiten conocer evolución, exposición, cumplimiento y eficacia de controles.

1.17.1 KRI — Key Risk Indicators

Los KRI son métricas que permiten observar si un riesgo está **aumentando antes de que se materialice**.

KRI	Riesgo asociado	Umbral sugerido
Sistemas críticos con parches vencidos	Explotación de vulnerabilidades	Máximo 5%
Usuarios con accesos no revisados	Permisos excesivos	Máximo 10%
Intentos fallidos de autenticación	Ataques de fuerza bruta	Umbral según sistema
Tiempo de baja de usuarios	Acceso indebido tras desvinculación	Mismo día para sistemas críticos
Fallas de restauración de backups	Imposibilidad de recuperación	0 fallas no justificadas en sistemas críticos

1.17.2 Indicadores de gestión

Indicador	Qué permite observar
Porcentaje de usuarios capacitados	Alcance de formación en seguridad
Resultado de simulacros de phishing	Exposición humana real
Cantidad de incidentes reportados	Cultura de reporte y visibilidad
Tiempo medio de respuesta	Capacidad de reacción
Riesgos críticos sin tratamiento	Brechas que requieren acción directiva
Activos críticos inventariados	Nivel de visibilidad sobre lo que debe protegerse
Proveedores críticos evaluados	Control sobre terceros
Restauraciones probadas con éxito	Capacidad real de recuperación
Tiempo medio de corrección	Velocidad de respuesta correctiva
Hallazgos repetidos de auditoría	Debilidades estructurales

Los indicadores deben tener dueño, fuente, frecuencia de medición y umbral. Un número sin interpretación no mejora la gestión. Un indicador aislado puede ser engañoso.

1.18 Escenarios de riesgo

Un escenario de riesgo describe una situación concreta en la cual un riesgo se materializa. Sirve para hacer más comprensible el análisis, especialmente ante audiencias no técnicas.

Elemento	Pregunta
Amenaza	¿Qué actor o evento genera el riesgo?
Vulnerabilidad	¿Qué debilidad permite que ocurra?
Activo afectado	¿Qué sistema, dato o proceso queda comprometido?

Elemento	Pregunta
Consecuencia	¿Qué impacto tendría?
Controles	¿Qué medidas reducen el riesgo?

Escenario: fraude por modificación de CBU

Un empleado recibe un correo que aparenta provenir de un proveedor habitual. El mensaje solicita modificar el CBU para los próximos pagos. La organización no exige verificación por canal alternativo y el cambio se realiza en el sistema.

Elemento	Análisis
Riesgo	Fraude financiero por modificación indebida de datos bancarios
Vulnerabilidad	Ausencia de verificación independiente
Impacto	Transferencia a cuenta incorrecta y pérdida económica
Control preventivo	Doble aprobación y confirmación telefónica a contacto registrado
Control detectivo	Reporte automático de cambios en datos bancarios
Control correctivo	Bloqueo del pago y revisión de operaciones pendientes

El escenario permite ver que el problema no es solo tecnológico: intervienen correo, proceso de pagos, datos de proveedores, controles contables y responsabilidad administrativa.

1.19 Evaluación costo-beneficio de controles

Implementar controles tiene un costo que debe compararse con el beneficio producido, medido como reducción de la pérdida esperada.

Beneficio del control = Pérdida esperada sin control − Pérdida esperada con control

Concepto	Valor
Pérdida esperada sin control	USD 90.000
Pérdida esperada con control	USD 24.000
Beneficio del control	USD 66.000
Costo anual del control	USD 25.000
Beneficio neto estimado	**USD 41.000**

En este caso, el control se justifica económicamente porque el beneficio supera el costo. Sin embargo, existen controles que pueden implementarse aunque no resulten rentables en términos estrictamente financieros, por exigencias legales, contractuales, regulatorias o reputacionales.

1.20 Pérdida esperada, BIA, RTO y RPO

Concepto	Significado	Uso administrativo
Pérdida esperada	Probabilidad × impacto económico	Comparar riesgos y justificar controles
BIA	Análisis de impacto en el negocio	Priorizar procesos críticos
RTO	Tiempo máximo aceptable de interrupción	Definir plazo de recuperación del sistema

Concepto	Significado	Uso administrativo
RPO	Máxima pérdida aceptable de datos medida en tiempo	Definir frecuencia de respaldo

Ejemplo integrado: si el sistema de facturación genera pérdidas de USD 18.000 por hora de interrupción y la organización define un RTO de 2 horas, los controles de continuidad deben permitir recuperar el servicio dentro de ese plazo. Si el esquema actual demora 8 horas, existe una brecha de continuidad que debe resolverse. Si el RPO es de 1 hora, los respaldos deben permitir recuperar datos con una antigüedad máxima de una hora.

1.21 Cinco dimensiones del riesgo organizacional en TI

Para ordenar el análisis desde la administración y la tecnología, se pueden considerar cinco dimensiones integradas. Estas dimensiones no funcionan de manera aislada: un incidente puede comenzar por falta de capacitación, agravarse por permisos excesivos, no detectarse por ausencia de monitoreo y terminar en incumplimiento normativo.

Dimensión	Enfoque	Pregunta central
Concientización y capacitación	Conducta de las personas	¿Los usuarios comprenden los riesgos y saben cómo actuar?
Aspectos de personal	Ciclo de vida del usuario	¿Los accesos se asignan, modifican y revocan correctamente?
Administración del riesgo	Identificación y tratamiento	¿Los riesgos se miden y gestionan con criterios formales?
Estrategia de seguridad	Prioridades y controles	¿Existe una dirección clara para proteger la información?

Dimensión	Enfoque	Pregunta central
Políticas y regulación	Reglas y cumplimiento	¿La organización cuenta con normas, evidencias y responsabilidades?

1.21.1 Concientización y capacitación

La concientización busca que las personas comprendan los riesgos. La capacitación busca que sepan cómo actuar. Ambas son necesarias y deben ser **periódicas, medibles y diferenciadas por rol**.

Riesgo por falta de capacitación	Consecuencia	Control recomendado
Abrir correos falsos	Robo de credenciales	Simulaciones de phishing y formación práctica
Compartir contraseñas	Acceso no autorizado	Política de credenciales y MFA
No reportar incidentes	Demora en la respuesta	Canal de reporte claro y sin sanción por buena fe
Usar aplicaciones no autorizadas	Fuga de datos	Política de software permitido y monitoreo
Clasificar mal información	Exposición de datos sensibles	Capacitación sobre niveles de información

1.21.2 Aspectos de personal — Ciclo de vida del usuario

Cada empleado, proveedor o usuario externo con acceso a sistemas representa una identidad digital que debe tener permisos adecuados, limitados, monitoreados y revocados cuando deja de corresponder.

Momento del ciclo laboral	Riesgo	Control
Ingreso	Permisos excesivos desde el inicio	Alta según perfil aprobado
Permanencia	Acumulación de privilegios	Revisión periódica de accesos
Cambio de puesto	Conservación de permisos anteriores	Modificación formal del perfil
Tareas críticas	Concentración de funciones incompatibles	Segregación de funciones
Desvinculación	Usuario activo después de la baja	Offboarding inmediato y documentado

La **segregación de funciones** es clave: en un proceso de pagos, no debería ser la misma persona quien crea el proveedor, aprueba la factura, modifica el CBU y ejecuta la transferencia.

1.21.3 Estrategia de seguridad

Una estrategia de seguridad define qué se protege, por qué, con qué prioridad, con qué recursos, quién es responsable y cómo se mide el resultado.

Componente	Función
Inventario de activos	Saber qué sistemas, datos y servicios existen
Clasificación de información	Determinar sensibilidad y tratamiento de los datos
Responsables definidos	Asignar dueños de procesos y activos
Controles técnicos	Proteger, detectar y recuperar

Componente	Función
Controles administrativos	Formalizar políticas, procedimientos y evidencias
Respuesta ante incidentes	Definir cómo actuar ante eventos de seguridad
Continuidad del negocio	Mantener procesos críticos ante interrupciones
Mejora continua	Revisar incidentes, indicadores y controles

1.21.4 Políticas y regulación

Política	Finalidad
Uso aceptable	Regular el uso de equipos, correo, internet y sistemas
Contraseñas y MFA	Establecer requisitos de autenticación
Clasificación de información	Definir niveles de sensibilidad
Trabajo remoto	Regular accesos fuera de la oficina
Alta, modificación y baja de usuarios	Controlar el ciclo de vida de accesos
Proveedores	Exigir requisitos de seguridad a terceros
Respuesta ante incidentes	Definir roles y pasos de actuación
Backup y recuperación	Establecer copias, pruebas y tiempos de restauración

Una política sin comunicación no cambia conductas. Una política sin evidencia no puede auditarse. Una política sin responsable no se sostiene en el tiempo.

1.22 La seguridad como sistema organizacional

La seguridad no debe pensarse solo como un conjunto de herramientas técnicas, ni solo como un conjunto de políticas. Debe verse como un **sistema organizacional** que combina todas las dimensiones de manera articulada.

Dimensión	Ejemplo en TI
Políticas	Política de contraseñas, uso aceptable, clasificación de información
Procesos	Gestión de accesos, vulnerabilidades, incidentes y cambios
Tecnología	Firewalls, EDR, cifrado, SIEM
Monitoreo	Alertas, tableros de riesgo, revisión de logs
Capacitación	Concientización frente a phishing y uso seguro
Gobierno	Comité, responsables, métricas y revisión de riesgos
Cumplimiento	Adecuación a normas y obligaciones regulatorias

Esto recuerda que la seguridad debe pensarse en su totalidad. No es razonable gestionar el riesgo tecnológico solo con herramientas, ni solo con políticas, ni solo con personas. Se necesita una combinación articulada.

1.23 El protector y la protección integral

La gestión de riesgos en profundidad desplaza la atención desde el “qué se protege” hacia el “quién protege” y “con qué capacidades”.

En TI, el protector puede ser: un equipo de seguridad, un administrador de sistemas, un auditor, un comité de riesgos, un responsable funcional o un proveedor especializado.

Capacidad del protector	Aplicación
Conocimiento técnico	Entender sistemas, redes, datos y controles
Conocimiento del negocio	Saber qué procesos son críticos
Capacidad de respuesta	Actuar ante alertas o incidentes
Autoridad	Poder tomar decisiones o escalar problemas
Ética y confiabilidad	Administrar información y accesos sensibles
Comunicación	Explicar riesgos a técnicos y no técnicos
Actualización	Aprender nuevas amenazas y controles

La **protección integral** incluye muchas dimensiones. Un control técnico puede fracasar si no hay procedimientos. Un buen procedimiento puede fallar si el equipo no está capacitado. Una organización puede tener personas preparadas y aun así verse afectada si su proveedor carece de medidas adecuadas.

Componente	Ejemplo en TI
Capacitación	Entrenar al personal en detección de correos falsos
Procedimientos	Definir cómo dar de baja accesos al desvincular empleados
Capacidades técnicas	Herramientas de monitoreo y respuesta

Componente	Ejemplo en TI
Conciencia	Cultura de reporte de incidentes
Terceros	Evaluación de seguridad de proveedores
Cumplimiento legal	Protección de datos personales y conservación de evidencia
Continuidad	Planes de respaldo y recuperación

La protección no debe verse como un muro único, sino como un conjunto de capas complementarias.

1.24 Resiliencia y continuidad del negocio

La **resiliencia** es la capacidad de anticipar, resistir, responder y recuperarse. Una gestión de riesgos en profundidad contribuye directamente a ella.

Capacidad de resiliencia	Aplicación en TI
Anticipar	Identificar activos, amenazas y contextos
Resistir	Implementar controles preventivos
Detectar	Monitorear actividad y anomalías
Responder	Activar procedimientos y responsabilidades
Recuperar	Restaurar servicios y datos
Aprender	Incorporar lecciones del incidente

La continuidad del negocio también depende de esta mirada. Si un sistema crítico cae, la organización debe conocer el activo afectado, sus exposiciones, sus vulnerabilidades, sus amenazas probables y sus alternativas de recuperación.

1.25 El contexto como variable del riesgo

El riesgo nunca existe en el vacío. Todo riesgo está inmerso en un contexto que puede agravar o reducir su nivel de criticidad. Un mismo activo puede tener distinto nivel de criticidad según el entorno.

Variable contextual	Impacto posible en el riesgo
Sector	No enfrenta lo mismo una pyme comercial que un banco o un hospital
Regulación	Algunas industrias tienen mayores exigencias normativas
Geografía	Puede cambiar conectividad, amenazas físicas o soberanía de datos
Tipo de operación	No es igual un sistema interno que un servicio digital público
Dependencia tecnológica	Cuanto mayor es la dependencia, mayor suele ser la criticidad
Cadena de suministro	Riesgos compartidos con terceros y servicios cloud
Madurez organizacional	Cambia la capacidad de prevenir, detectar y responder

1.26 Responsabilidades por área

La gestión de riesgos de TI es una responsabilidad organizacional compartida.

Área	Responsabilidad frente al riesgo
Alta dirección	Definir apetito de riesgo, prioridades y recursos
Administración	Alinear controles con procesos, costos y responsabilidades
TI	Implementar controles técnicos, monitoreo y recuperación
Recursos Humanos	Coordinar altas, cambios, bajas y capacitación
Legal	Revisar cumplimiento, contratos y obligaciones regulatorias
Auditoría	Evaluar controles, evidencias y cumplimiento
Usuarios	Cumplir políticas y reportar incidentes
Proveedores	Respetar requisitos de seguridad y confidencialidad

La dirección no necesita configurar firewalls ni administrar servidores, pero sí debe exigir reportes, aprobar políticas, asignar presupuesto y conocer los riesgos críticos que afectan al negocio.

1.27 Cultura organizacional como control

La cultura organizacional es un **control transversal**. Una organización puede tener buenas herramientas y seguir siendo vulnerable si las personas no reportan incidentes, comparten contraseñas, omiten procedimientos o consideran que la seguridad es una molestia ajena al negocio.

Una cultura de seguridad madura promueve conductas concretas: - Reportar correos sospechosos. - No compartir credenciales. - Verificar instrucciones de pago por canales independientes. - Respetar los niveles de autorización. - Consultar antes de usar herramientas externas. - Proteger dispositivos y documentos. - Aceptar los controles como parte del trabajo normal.

La cultura no reemplaza a los controles técnicos, pero mejora su eficacia. Un usuario capacitado y comprometido puede ser una primera línea de defensa. Un usuario desinformado puede convertirse en el punto de entrada de un incidente.

1.28 Errores frecuentes en la gestión de riesgos

Error	Consecuencia
No inventariar activos	Se dejan sin protección recursos críticos
Concentrarse solo en vulnerabilidades técnicas	No se revisan usuarios, procesos, terceros o contratos
No revisar la exposición	Se subestiman accesos y superficies de ataque
No identificar amenazas adecuadamente	Se diseñan controles insuficientes
Ignorar el contexto	La evaluación se vuelve abstracta y poco útil
No definir protectores claros	Si nadie es responsable de un control, ese control tiende a fallar
Asumir que una herramienta equivale a protección	Una solución tecnológica sin procedimiento, monitoreo ni capacitación tiene valor limitado

Error	Consecuencia
Separar riesgo, seguridad y continuidad	Estas funciones están conectadas: una falla de seguridad puede convertirse en un problema de continuidad y reputación
No probar backups ni controles	Un backup no probado no garantiza recuperación; un control sin evidencia no puede demostrarse
Aceptar riesgos sin documentar	Una aceptación sin fecha de revisión se convierte en una debilidad permanente

1.29 Casos integradores

1.29.1 Caso 1 — Phishing a personal administrativo

Un usuario del área administrativa recibe un correo que simula provenir del banco corporativo. El mensaje solicita validar credenciales. El usuario ingresa sus datos en un sitio falso y el atacante intenta acceder al sistema de pagos.

Aspecto	Análisis
Riesgo	Acceso indebido a sistema financiero
Fuente	Ingeniería social y error humano
Vulnerabilidad	Falta de capacitación o ausencia de MFA
Impacto	Transferencias no autorizadas y pérdida económica
Controles	Capacitación, MFA, filtro de correo, monitoreo y doble aprobación

1.29.2 Caso 2 — Baja tardía de usuario

Un empleado se desvincula, pero su cuenta permanece activa durante dos semanas.

Aspecto	Análisis
Riesgo	Acceso indebido posterior a la desvinculación
Fuente	Debilidad en proceso de personal
Vulnerabilidad	Falta de integración entre RR.HH. y TI
Impacto	Consulta, modificación o eliminación de información
Controles	Offboarding formal, baja automática, reporte de usuarios activos

1.29.3 Caso 3 — Sistema crítico sin continuidad

El sistema de facturación depende de un único servidor local. No existe prueba reciente de restauración ni procedimiento alternativo.

Aspecto	Análisis
Riesgo	Interrupción operativa prolongada
Fuente	Falla tecnológica o evento físico
Vulnerabilidad	Ausencia de redundancia y backups probados
Impacto	Imposibilidad de facturar, cobrar y atender clientes
Controles	BIA, RTO, RPO, backups probados, redundancia y contingencia

1.29.4 Caso 4 — Shadow IT: uso de aplicación no autorizada

Un área sube contratos y bases de clientes a una herramienta gratuita en la nube para compartir archivos con proveedores, sin pasar por TI.

Aspecto	Análisis
Riesgo	Fuga de información confidencial
Fuente	Shadow IT y falta de política
Vulnerabilidad	Ausencia de control sobre herramientas externas
Impacto	Exposición de datos, incumplimiento contractual o legal
Controles	Política de software permitido, capacitación, DLP

1.29.5 Caso 5 — ERP en empresa mediana (ejemplo integrador de las cuatro estrategias)

Riesgo	Prob.	Impacto	Nivel	Tratamiento	Controles
Usuarios con permisos excesivos	4	4	16 Alto	**Mitigar**	Perfiles por función, revisión mensual, baja inmediata, aprobación formal
Indisponibilidad del proveedor cloud	2	5	10 Alto	**Transferir + mitigar**	SLA, plan de continuidad, exportación periódica,

Riesgo	Prob.	Impacto	Nivel	Tratamiento	Controles
					procedimiento alternativo
Carga errónea de precios	3	3	9 Medio	**Mitigar**	Validaciones automáticas, doble revisión, aprobación de listas
Módulo que recolecta datos innecesarios	3	4	12 Alto	**Evitar**	Desactivar el módulo o modificar el proceso
Interrupción menor fuera de horario	2	1	2 Bajo	**Aceptar**	Documentar la aceptación; verificar que no afecta cierres contables

Este ejemplo muestra que una misma organización puede aplicar las cuatro estrategias de tratamiento en simultáneo. La decisión depende del riesgo concreto, no de una preferencia general.

1.30 Ideas clave

- La información debe tratarse como un **activo crítico** de la organización porque sostiene operaciones, decisiones, obligaciones legales y continuidad del negocio.
- Los riesgos de TI son **riesgos de negocio**. Sus consecuencias son administrativas, económicas, legales y reputacionales, aunque muchas soluciones sean técnicas.
- La **tríada CIA** permite ordenar el análisis de seguridad según confidencialidad, integridad y disponibilidad.
- Un riesgo surge de la intersección entre **activo, exposición, vulnerabilidad y amenaza**. Los controles actúan sobre las vulnerabilidades.
- El **riesgo inherente** no desaparece con los controles: se reduce al **riesgo residual**. La organización debe decidir conscientemente qué nivel de riesgo residual es aceptable: esa decisión es el **apetito de riesgo**.
- Las cuatro estrategias de tratamiento —**evitar, mitigar, transferir y aceptar**— no son equivalentes. Cada una aplica según la naturaleza del riesgo, el proceso afectado, el costo del control y la tolerancia organizacional.
- **Transferir** el riesgo no elimina la responsabilidad. Un contrato, un seguro o un SLA distribuye consecuencias, pero la organización sigue siendo responsable de evaluar, controlar y auditar a sus proveedores.
- **Aceptar** un riesgo no es ignorarlo. Requiere documentación formal: quién aprueba, qué se acepta, por qué y cuándo se revisará.
- La **segregación de funciones** conecta la seguridad informática con el control interno administrativo, especialmente en procesos sensibles como pagos, altas de proveedores y modificaciones de datos bancarios.
- La **concientización y la capacitación** reducen riesgos humanos, pero deben ser periódicas, medibles y diferenciadas por rol.

- La gestión del ciclo de vida del usuario —**alta, permanencia, cambio y baja**— es una responsabilidad compartida entre Recursos Humanos y TI.
- Los **KRI** permiten anticipar aumentos de exposición antes de que el riesgo se materialice.
- Un **backup no probado** no garantiza recuperación. Un **control sin evidencia** no puede demostrarse. Un **plan sin responsable** no se ejecuta.
- La **defensa en profundidad** evita depender de un único control y permite reducir el impacto cuando una barrera falla.
- La **cultura organizacional** es un control transversal que mejora la eficacia de todos los controles técnicos y administrativos.
- La gestión del riesgo de TI requiere **gobierno, evidencia, responsables, seguimiento e integración** con auditoría y dirección.

1.31 Preguntas de evaluación

1. ¿Por qué la información debe considerarse un activo crítico dentro de una organización? Incluya ejemplos vinculados con administración, contabilidad o procesos comerciales.
2. Explique la tríada CIA y proporcione un ejemplo organizacional para cada uno de los tres principios.
3. ¿Qué diferencia existe entre activo, exposición, vulnerabilidad y amenaza? Proporcione un ejemplo concreto para cada componente en el contexto de un sistema de gestión empresarial.
4. ¿Por qué los riesgos de TI no deben tratarse como problemas exclusivamente técnicos?
5. Identifique cuatro fuentes de riesgo en el manejo de la información y proponga un control para cada una.

6. ¿Qué diferencia existe entre análisis cualitativo y análisis cuantitativo del riesgo? ¿Cuándo conviene usar cada uno?
7. Calcule la pérdida esperada de un riesgo cuya probabilidad anual es del 20% y cuyo impacto estimado es de USD 100.000.
8. Un sistema de pagos tiene probabilidad 4 e impacto 5. ¿Cuál es su nivel de riesgo? ¿Qué tratamiento corresponde según la matriz y qué controles específicos podrían aplicarse?
9. ¿Qué diferencia existe entre riesgo inherente, riesgo residual y riesgo aceptado? ¿Qué papel cumple el apetito de riesgo en esa distinción?
10. ¿Qué significa apetito de riesgo y por qué debe traducirse en criterios operativos concretos?
11. En qué casos una organización debería **evitar** un riesgo en lugar de mitigarlo. Proporcione dos ejemplos.
12. ¿Por qué un contrato con un proveedor cloud no elimina completamente el riesgo? ¿Qué elementos debe incluir ese contrato para que la transferencia sea efectiva?
13. ¿Qué condiciones deben cumplirse para que la aceptación de un riesgo sea una decisión válida y no una omisión de gestión?
14. Clasifique los siguientes controles como preventivos, detectivos, correctivos o recuperatorios: MFA, logs de auditoría, bloqueo de cuenta comprometida, backup restaurable.
15. ¿Qué es la segregación de funciones y por qué es relevante en un proceso de pagos a proveedores?
16. Explique cómo se relaciona el ciclo de vida del empleado con la gestión de accesos a sistemas.

17. ¿Cuál es la diferencia entre concientización y capacitación? ¿Por qué ambas son necesarias y qué riesgos genera no tenerlas?
18. ¿Qué información debe incluir un registro de riesgos para ser útil como herramienta de gestión?
19. ¿Quién debe ser el dueño de un riesgo y por qué no siempre debe ser una persona del área técnica?
20. ¿Qué son los KRI y cómo se diferencian de los indicadores de desempeño tradicionales?
21. ¿Qué elementos debe incluir un escenario de riesgo para que sea comprensible ante un comité de dirección?
22. Explique cómo se evalúa el costo-beneficio de un control de seguridad. ¿Cuándo puede justificarse implementar un control que no resulta rentable en términos estrictamente financieros?
23. ¿Qué relación existe entre BIA, RTO, RPO y continuidad del negocio?
24. ¿Por qué la cultura organizacional puede considerarse un control de seguridad? ¿Qué diferencia hace una cultura madura respecto de una indiferente al riesgo?
25. ¿Qué responsabilidades tienen la alta dirección, TI, Recursos Humanos, Legal y Auditoría frente a los riesgos de información?
26. ¿Por qué no basta con identificar solo vulnerabilidades técnicas para gestionar el riesgo en profundidad?
27. Analice el caso de modificación fraudulenta de CBU e identifique controles preventivos, detectivos y correctivos.
28. Diseñe una matriz simple con tres riesgos de una empresa mediana, calcule su nivel y proponga un tratamiento para cada uno.

1.32 Glosario

Término o sigla	Traducción / Explicación
API	*Application Programming Interface*. Interfaz de programación de aplicaciones. Permite que distintos sistemas intercambien datos u operaciones.
Asset	Activo. Recurso con valor para la organización que debe protegerse. Puede ser digital, físico, humano, de conocimiento o de proceso.
Audit Log	Registro de auditoría. Registro cronológico e inmutable de las acciones realizadas en un sistema: quién accedió, qué modificó y cuándo.
Awareness	Concientización. Proceso destinado a que las personas comprendan riesgos y responsabilidades de seguridad.
Backup	Copia de respaldo. Solo tiene valor si puede restaurarse exitosamente. Un backup no probado no garantiza recuperación.
BCP	*Business Continuity Plan*. Plan de continuidad del negocio. Define cómo seguir operando ante interrupciones relevantes.
BIA	*Business Impact Analysis*. Análisis de impacto en el negocio. Permite identificar procesos críticos, impactos de interrupción y prioridades de recuperación.
CASB	*Cloud Access Security Broker*. Intermediario de seguridad de acceso a la nube. Ayuda a controlar el uso de servicios en la nube.

Término o sigla	Traducción / Explicación
CBU	Clave Bancaria Uniforme. Identificador bancario argentino utilizado para transferencias. Relevante por su relación con riesgos de fraude financiero.
CIA	*Confidentiality, Integrity and Availability*. Confidencialidad, Integridad y Disponibilidad. Tríada básica de la seguridad de la información.
COBIT	*Control Objectives for Information and Related Technologies*. Marco de gobierno y gestión de TI.
CRM	*Customer Relationship Management*. Sistema para administrar clientes, oportunidades y relaciones comerciales.
Defense in Depth	Defensa en profundidad. Estrategia que combina varias capas de control para reducir riesgos y evitar dependencia de una única barrera.
DLP	*Data Loss Prevention*. Prevención de pérdida de datos. Conjunto de controles para evitar fugas de información sensible.
DRP	*Disaster Recovery Plan*. Plan de recuperación ante desastres. Define cómo recuperar sistemas e infraestructura luego de un evento grave.
EDR	*Endpoint Detection and Response*. Detección y respuesta en dispositivos finales. Herramienta para monitorear equipos y responder ante amenazas.

Término o sigla	Traducción / Explicación
ERM	*Enterprise Risk Management*. Gestión de riesgos empresariales. Enfoque integral que vincula riesgos con objetivos estratégicos.
ERP	*Enterprise Resource Planning*. Sistema integrado para gestionar procesos centrales del negocio (compras, ventas, inventario, contabilidad).
Expected Loss	Pérdida esperada. Estimación resultante de multiplicar probabilidad por impacto económico.
Exposure	Exposición. Condición por la cual un activo puede quedar al alcance del daño.
Firewall	Cortafuegos. Control que permite o bloquea tráfico de red según reglas definidas.
Hardening	Endurecimiento. Configuración segura de un sistema para reducir superficie de ataque.
Heat Map	Mapa de calor. Representación visual de la matriz de riesgos según probabilidad e impacto. Útil para presentar riesgos a la dirección.
Inherent Risk	Riesgo inherente. Nivel de riesgo existente antes de aplicar controles.
IS	*Information System*. Sistema de Información. Combinación de personas, procesos, datos y tecnología orientada a producir información útil.

Término o sigla	Traducción / Explicación
IT / TI	*Information Technology*. Tecnologías de la Información. Conjunto de recursos tecnológicos para procesar, almacenar, transmitir y proteger información.
KPI	*Key Performance Indicator*. Indicador clave de desempeño. Mide rendimiento de procesos o actividades.
KRI	*Key Risk Indicator*. Indicador clave de riesgo. Señal temprana que permite monitorear si un riesgo está aumentando antes de materializarse.
Logs	Registros de actividad generados por sistemas, aplicaciones o dispositivos. Se usan para monitoreo, auditoría e investigación.
Malware	*Malicious Software*. Software malicioso diseñado para dañar, espiar, interrumpir o tomar control de sistemas.
MFA	*Multi-Factor Authentication*. Autenticación multifactor. Exige más de un factor para validar identidad al ingresar a un sistema.
NIST RMF	*National Institute of Standards and Technology Risk Management Framework*. Marco de gestión del riesgo del NIST.
Offboarding	Proceso formal de desvinculación. Incluye baja de accesos, devolución de equipos y cierre de credenciales.
Phishing	Técnica de engaño mediante correos, mensajes o sitios falsos para obtener credenciales o información sensible.

Término o sigla	Traducción / Explicación
Ransomware	Malware que cifra o bloquea información y exige una condición para restaurar el acceso. Puede paralizar operaciones completas y destruir backups no aislados.
Residual Risk	Riesgo residual. Nivel de riesgo que permanece después de implementar controles. Debe ser aceptable según el apetito de la organización.
Restore Test	Prueba de restauración. Verificación periódica de que una copia de seguridad puede recuperarse exitosamente dentro del tiempo requerido.
Risk Acceptance	Aceptación del riesgo. Decisión formal de no implementar controles adicionales, documentando la justificación y la fecha de revisión.
Risk Appetite	Apetito de riesgo. Nivel de riesgo que la organización está dispuesta a aceptar para cumplir sus objetivos. Debe traducirse en criterios operativos concretos.
Risk Avoidance	Evitación del riesgo. Decisión de no iniciar, discontinuar o modificar una actividad para eliminar la exposición al riesgo.
Risk Management	Gestión del riesgo. Proceso de identificación, análisis, valoración, tratamiento y monitoreo de riesgos.
Risk Mitigation	Mitigación del riesgo. Implementación de controles para disminuir la probabilidad de ocurrencia, el impacto, o ambos.
Risk Owner	Dueño del riesgo. Persona responsable de gestionar un riesgo específico. No siempre es del área técnica.

Término o sigla	Traducción / Explicación
Risk Register	Registro de riesgos. Documento o sistema donde se consolidan riesgos, controles, responsables y seguimiento.
Risk Tolerance	Tolerancia al riesgo. Margen aceptable de variación respecto del apetito de riesgo definido.
Risk Transfer / Sharing	Transferencia del riesgo. Traslado total o parcial del impacto a un tercero mediante contratos, seguros o acuerdos. No elimina la responsabilidad de la organización.
RPO	*Recovery Point Objective*. Punto objetivo de recuperación. Indica cuánta información puede perderse como máximo, medida en tiempo.
RTO	*Recovery Time Objective*. Tiempo objetivo de recuperación. Indica cuánto tiempo máximo puede estar interrumpido un sistema.
Security	Seguridad. Sistema de protección frente a amenazas intencionales o accidentales sobre sistemas, datos y tecnologías.
Shadow IT	Uso de tecnología no aprobada formalmente por el área de TI. Puede incluir aplicaciones, servicios en la nube o dispositivos.
SIEM	*Security Information and Event Management*. Gestión de eventos e información de seguridad. Centraliza logs y genera alertas.
SLA	*Service Level Agreement*. Acuerdo de nivel de servicio. Define compromisos medibles sobre disponibilidad, tiempos de respuesta y calidad del servicio.

Término o sigla	Traducción / Explicación
SoD	*Segregation of Duties*. Segregación de funciones. Principio de control interno que evita que una misma persona concentre todas las etapas críticas de un proceso.
Threat	Amenaza. Evento o condición capaz de causar daño a un activo de información. Puede ser externa o interna, intencional o accidental.
Training	Capacitación. Formación práctica para que las personas sepan cómo actuar ante riesgos.
UPS	*Uninterruptible Power Supply*. Sistema de alimentación ininterrumpida. Mantiene energía temporal ante cortes eléctricos.
VPN	*Virtual Private Network*. Red privada virtual. Medio seguro para acceder remotamente a recursos organizacionales.
Vulnerability	Vulnerabilidad. Debilidad en un sistema, proceso o práctica que puede ser explotada por una amenaza.
Zero Day	Vulnerabilidad no conocida públicamente o sin corrección disponible al momento del ataque.