Controles de Seguridad en los Sistemas de Información

1.1 Introducción

La seguridad de la información no puede reducirse a una contraseña, a un antivirus o a una cámara de vigilancia. En una organización real, la seguridad se construye mediante un conjunto coordinado de controles físicos, lógicos, administrativos y humanos.

Estos controles buscan proteger los activos de información frente a amenazas internas y externas: accesos no autorizados, errores humanos, sabotajes, filtraciones de datos, fallas técnicas, robo de equipos, interrupciones del servicio, ataques informáticos o incumplimientos normativos.

Desde la mirada de la administración, el tema no es solamente técnico. Un control puede ser una política, una autorización, una conciliación, una revisión de usuarios, una separación de funciones, una capacitación, un registro de auditoría, un procedimiento de baja, una prueba de restauración o un plan de continuidad. Los controles forman parte del sistema de control interno de la organización y permiten reducir riesgos, ordenar responsabilidades, proteger procesos, preservar evidencia, mejorar la trazabilidad y sostener la continuidad operativa.

Idea central: la seguridad no depende de un único control, sino de la combinación inteligente de medidas físicas, lógicas, administrativas y culturales. Un sistema seguro no es aquel que nunca enfrenta problemas, sino aquel que cuenta con controles adecuados para prevenirlos, detectarlos, corregirlos y recuperarse cuando ocurren.

1.2 La tríada CIA: confidencialidad, integridad y disponibilidad

Los controles de seguridad buscan preservar tres principios fundamentales, conocidos como la tríada **CIA** (*Confidentiality, Integrity, Availability*).

Principio	Significado	Ejemplo organizacional	Riesgo que intenta reducir
Confidencialidad	La información solo debe ser accesible para personas autorizadas	Un legajo de personal no debe estar disponible para cualquier usuario	Acceso no autorizado o fuga de datos
Integridad	La información debe mantenerse completa, correcta y no alterada indebidamente	Una factura no debe modificarse sin autorización	Error, fraude o manipulación
Disponibilidad	Los sistemas y datos deben estar accesibles cuando se los necesita	El sistema de facturación debe funcionar durante la jornada comercial	Interrupción del servicio o pérdida operativa

Un mismo evento puede afectar más de un principio. Un ransomware puede afectar la disponibilidad porque impide el acceso, la confidencialidad si el atacante copió datos antes de cifrarlos, y la integridad si los archivos fueron dañados.

1.3 El concepto administrativo de control

Un control de seguridad es una medida organizada que busca reducir un riesgo. Para que sea útil como herramienta de gestión debe tener cinco elementos:

Elemento del control	Pregunta administrativa
Objetivo	¿Qué riesgo se busca reducir?
Responsable	¿Quién debe aplicarlo, supervisarlo o aprobarlo?

Elemento del control	Pregunta administrativa
Procedimiento	¿Cómo se ejecuta el control?
Evidencia	¿Qué registro demuestra que el control se aplicó?
Revisión	¿Cómo se verifica si funciona correctamente?

Ejemplo: la revisión trimestral de usuarios activos es un control. Su objetivo es detectar accesos innecesarios. El responsable puede ser cada jefe de área con soporte de TI. El procedimiento consiste en enviar listados, confirmar permisos y solicitar bajas. La evidencia puede ser una planilla firmada o un reporte del sistema. La revisión puede realizarse por auditoría interna.

Un control sin evidencia es difícil de auditar. Un control sin responsable suele aplicarse de manera irregular. Un control sin revisión puede quedar obsoleto.

1.4 Clasificación general de controles

Según el momento en que actúan y su finalidad, los controles se clasifican en cuatro tipos:

Tipo de control	Momento en que actúa	Finalidad principal	Pregunta de gestión
Preventivo	Antes del evento	Evitar que ocurra un error, incidente o irregularidad	¿Cómo evito que ocurra?
Detectivo	Durante o después del evento	Identificar que algo ocurrió o está ocurriendo	¿Cómo me entero de que pasó?
Correctivo	Después de detectar el problema	Corregir la causa o el efecto de la falla	¿Cómo corrijo el error o daño?

Tipo de control	Momento en que actúa	Finalidad principal	Pregunta de gestión
Recuperatorio	Después de una interrupción significativa	Restaurar información, sistemas o procesos	¿Cómo restauro el servicio y continúo operando?

Esta clasificación permite comprender que la seguridad no se resuelve con un único tipo de medida. Una organización necesita prevenir, detectar, corregir y recuperarse. Ningún control preventivo es perfecto: los usuarios pueden cometer errores, los sistemas pueden fallar y las amenazas pueden cambiar.

Una organización que solo previene pero no detecta puede no advertir sus propias fallas. Una que detecta pero no corrige acumula problemas. Una que corrige pero no puede recuperar sus servicios críticos queda expuesta a interrupciones graves.

1.5 Controles preventivos

Los controles preventivos son la **primera línea de defensa**. Su objetivo es evitar que se produzcan eventos que afecten la confidencialidad, integridad o disponibilidad de los activos de información. Actúan antes del incidente y buscan reducir la probabilidad de errores, omisiones, accesos indebidos, fraudes, manipulaciones o fallas evitables.

Son especialmente relevantes cuando el impacto potencial es alto o cuando corregir el problema sería costoso. En administración, se vinculan con autorización previa, separación de funciones, validaciones, capacitación, restricciones y diseño adecuado de procesos.

Control preventivo	Riesgo que reduce
Autenticación multifactor (MFA)	Uso indebido de credenciales robadas
Separación de funciones	Fraude o abuso de permisos

Control preventivo	Riesgo que reduce
Doble aprobación	Operaciones críticas no autorizadas
Validaciones de datos	Carga de información incorrecta
Control físico de áreas críticas	Manipulación o robo de equipos
Políticas de uso aceptable	Conductas inseguras o no autorizadas
Capacitación preventiva	Errores por desconocimiento
Restricción de instalación de software	Malware o programas no autorizados
Clasificación de información	Tratamiento inadecuado de datos sensibles
Cifrado de dispositivos	Exposición de datos ante robo o pérdida
Formularios prenumerados	Omisiones o duplicaciones documentales
Firewalls	Tráfico de red no autorizado
Redundancia de componentes	Interrupciones por falla de un único componente

1.5.1 Ejemplos administrativos de controles preventivos

- Un cambio de cuenta bancaria de proveedor debe requerir solicitud documentada, validación de documentación, doble aprobación y confirmación por canal independiente. Este control previene pagos indebidos.
- Un usuario del área de compras no debería poder crear proveedores, modificar cuentas bancarias y aprobar pagos. La separación de funciones previene fraude y reduce errores.
- Un sistema de facturación debe validar datos obligatorios, CUIT, fechas, importes y reglas comerciales. Las validaciones previenen operaciones incorrectas.

1.5.2 Criterios para diseñar controles preventivos

Los controles preventivos deben ser **proporcionales**. Si son excesivos, pueden paralizar la operación. Si son débiles, no reducen el riesgo.

Criterio	Pregunta de gestión
Criticidad del activo	¿Qué valor tiene la información o el sistema protegido?
Impacto potencial	¿Qué ocurriría si el control falla?
Frecuencia de la operación	¿El control se aplicará todos los días o solo en casos excepcionales?
Costo operativo	¿Genera demoras razonables o excesivas?
Evidencia	¿Permite demostrar que fue aplicado?
Excepciones	¿Qué ocurre si el control no puede aplicarse temporalmente?

1.6 Controles detectivos

Los controles detectivos permiten identificar eventos, errores, accesos indebidos o irregularidades. No siempre impiden que el hecho ocurra, pero permiten conocerlo y actuar. Su valor depende de la **oportunidad**: detectar un acceso indebido en pocos minutos tiene un efecto muy distinto que detectarlo meses después.

Control detectivo	Qué permite identificar
Logs de acceso	Quién ingresó, cuándo y desde dónde
Pistas de auditoría	Qué operación se realizó y qué dato cambió

Control detectivo	Qué permite identificar
Conciliaciones	Diferencias entre registros o sistemas
Totales de control	Desvíos en cantidades o importes procesados
Reportes de excepción	Operaciones fuera de parámetros normales
Monitoreo de recursos	Uso anómalo de CPU, memoria, red o almacenamiento
Alertas de seguridad	Intentos fallidos, accesos inusuales o cambios críticos
IDS	Patrones sospechosos de intrusión
Revisión periódica de usuarios	Permisos indebidos o cuentas inactivas
Cámaras y registros físicos	Ingresos no habituales o no autorizados
Controles de secuencia	Saltos, duplicaciones u omisiones
Dígito verificador	Errores en códigos o números

1.6.1 Logs y pistas de auditoría

Los logs son registros automáticos de actividad. Las pistas de auditoría permiten reconstruir una operación. En un sistema administrativo, una pista de auditoría debería indicar usuario, fecha, hora, operación, dato anterior, dato nuevo y autorización asociada.

Operación	Evidencia esperada
Cambio de cuenta bancaria	Usuario, fecha, dato anterior, dato nuevo y aprobación

Operación	Evidencia esperada
Alta de usuario	Solicitante, aprobador, perfil asignado y fecha
Aprobación de pago	Usuario, monto, proveedor, fecha y regla aplicada
Eliminación de registro	Usuario, fecha, motivo y autorización
Exportación de datos	Usuario, volumen, destino y sistema utilizado

Un registro que nadie revisa tiene valor limitado. El control detectivo exige revisión, alertas o auditoría. La organización debe definir quién revisa, con qué frecuencia y qué se hace ante una anomalía.

1.6.2 Conciliaciones y controles cruzados

Las conciliaciones comparan registros de distintas fuentes: pagos emitidos contra movimientos bancarios, inventario físico contra inventario contable, facturas emitidas contra cobranzas, o usuarios activos contra nómina de personal. Los controles cruzados permiten detectar inconsistencias que no aparecen mirando un solo registro.

1.6.3 Controles con doble función

Algunos controles pueden cumplir más de una función:

Control	Función preventiva	Función detectiva
Capacitación en seguridad	Enseña buenas prácticas	Ayuda a reconocer y reportar incidentes
Políticas documentadas	Establecen reglas	Permiten comparar conducta real con la esperada

Control	Función preventiva	Función detectiva
Supervisión	Desalienta errores o abusos	Permite detectar desvíos
Monitoreo de accesos	Desalienta usos indebidos	Registra intentos o accesos sospechosos

1.7 Controles correctivos

Los controles correctivos buscan corregir una falla, error, desvío o vulnerabilidad detectada. Actúan después de identificar el problema. No deben limitarse a resolver el síntoma: deben corregir la **causa** para evitar que se repita.

Problema detectado	Control correctivo inmediato	Corrección de fondo
Usuario desvinculado activo	Bloquear cuenta	Integrar RR.HH. y TI para bajas automáticas
Permiso excesivo	Retirar privilegio	Revisar roles y aprobaciones
Dato erróneo	Corregir registro	Ajustar validación o capacitación
Software vulnerable	Aplicar parche	Implementar gestión de actualizaciones
Cambio no autorizado	Revertir modificación	Fortalecer gestión de cambios
Backup fallido	Reejecutar copia	Revisar monitoreo y responsabilidades

1.7.1 Corrección de datos con trazabilidad

En sistemas administrativos, toda corrección debe estar documentada con criterios de integridad:

Criterio	Aplicación
Trazabilidad	Registrar quién corrigió, cuándo y por qué
Autorización	Exigir aprobación cuando el dato sea sensible
Reversibilidad	Mantener posibilidad de reconstruir el estado anterior
Comunicación	Informar a áreas afectadas
Verificación	Confirmar que la corrección resolvió el problema

Corregir sin trazabilidad puede generar nuevos riesgos. Si se modifica una cuenta bancaria de proveedor sin conservar evidencia, la organización puede perder capacidad de auditoría.

Los controles correctivos suelen ser más costosos que los preventivos porque el problema ya ocurrió. Pueden requerir investigar qué pasó, identificar registros afectados, reprocesar operaciones, comunicar impactos y documentar la solución. Por eso, no deberían ser la única defensa de la organización.

1.8 Controles recuperatorios

Los controles recuperatorios permiten restaurar información, sistemas, servicios o procesos luego de una interrupción. No evitan el incidente, pero reducen su impacto. Se relacionan con continuidad operativa, recuperación ante desastres, redundancia, planes de contingencia y procedimientos alternativos.

Control recuperatorio	Finalidad
Backup	Recuperar datos perdidos o dañados
Restore probado	Verificar que la recuperación funciona realmente
Sitio alternativo	Operar desde otra ubicación o infraestructura
Redundancia	Mantener servicio ante falla de un componente
Soporte 7x24	Atender incidentes críticos en cualquier momento
Plan de contingencia	Definir acciones ante un evento específico
Plan de continuidad del negocio (BCP)	Sostener funciones críticas del negocio
Plan de recuperación ante desastres (DRP)	Recuperar infraestructura y sistemas
Procedimiento manual temporal	Operar durante una caída del sistema
Acuerdos de nivel de servicio (SLA)	Exigir tiempos de respuesta a proveedores

1.8.1 Backup y restore

Tener backups no equivale a poder recuperarse. La restauración debe probarse periódicamente.

Pregunta	Importancia
¿Qué se respalda?	Define el alcance de protección
¿Con qué frecuencia?	Determina la pérdida máxima posible
¿Dónde se guarda?	Evita pérdida simultánea con el sistema original

Pregunta	Importancia
¿Cómo se protege?	Evita robo, alteración o borrado
¿Cuándo se prueba?	Convierte expectativa en evidencia
¿Cuánto tarda restaurar?	Permite comparar con el RTO

Un backup guardado en el mismo servidor afectado puede perderse junto con los datos productivos. Un backup que nunca se prueba no demuestra capacidad de recuperación. Un backup accesible con las mismas credenciales comprometidas puede ser borrado por un atacante.

1.8.2 RTO, RPO y continuidad

Indicador	Pregunta que responde	Ejemplo
RTO	¿En cuánto tiempo debe volver el servicio?	Facturación debe recuperarse en 4 horas
RPO	¿Cuánta información puede perderse?	Se acepta perder como máximo 1 hora de datos
BCP	¿Cómo se sostiene el negocio?	Plan de continuidad del negocio
DRP	¿Cómo se recupera la tecnología?	Plan de recuperación ante desastres

Si una organización define un RPO de una hora, no puede respaldar solo una vez por día. Si define un RTO de cuatro horas, debe tener recursos, procedimientos y responsables capaces de recuperar dentro de ese plazo.

1.8.3 Procedimientos alternativos

Los controles recuperatorios también incluyen procedimientos manuales. Si cae el sistema de facturación, puede existir un procedimiento temporal para registrar operaciones y emitir comprobantes luego. Si un proveedor crítico queda indisponible,

puede usarse un proveedor secundario. **La improvisación no es un control recuperatorio**: el procedimiento alternativo debe estar documentado.

1.9 Integración: defensa en capas

Un control aislado rara vez alcanza. La protección eficaz combina los cuatro tipos de controles sobre cada proceso crítico.

Proceso	Preventivo	Detectivo	Correctivo	Recuperatorio
Pago a proveedores	Doble aprobación y segregación de funciones	Reporte de pagos inusuales y conciliación	Reversión o ajuste documentado	Restauración de base o procedimiento manual
Acceso a sistemas	MFA y mínimo privilegio	Logs e intentos fallidos	Retiro de permisos indebidos	Recuperación de cuentas o restauración de identidad
Sala técnica	Tarjeta, PIN y biometría	Cámara y registro de ingresos	Revocación de credenciales	Sitio alternativo o reposición de equipos
Datos críticos	Cifrado y clasificación	Monitoreo de descargas inusuales	Bloqueo de fuga y ajuste de permisos	Restore desde backup
Cambios de software	Gestión de cambios y pruebas	Revisión de logs y errores	Reversión del cambio	Restauración de versión anterior

Esta integración se conoce como **defensa en capas** o *defense in depth*: si un control falla, otros controles pueden limitar el daño, detectarlo o permitir recuperación.

1.10 Controles físicos

Los controles físicos protegen instalaciones, equipos, soportes, documentos, personas, áreas restringidas y recursos tecnológicos. Son esenciales porque los sistemas necesitan un entorno material para operar. Un sistema puede tener controles lógicos sólidos, pero seguir siendo vulnerable si una persona puede ingresar a una sala técnica, retirar un disco, desconectar un equipo o manipular un panel de comunicaciones.

Control físico	Finalidad
Puertas reforzadas y cerraduras	Restringir ingreso a áreas críticas
Tarjetas de proximidad y credenciales	Identificar usuarios y registrar ingresos
Molinetes o torniquetes	Ordenar y registrar ingreso de personas
CCTV y videovigilancia	Disuadir y registrar eventos
Sensores de movimiento	Detectar presencia no autorizada
Alarmas	Detectar intrusión o apertura indebida
Sensores ambientales	Detectar temperatura, humedad, humo o agua
Detectores y supresores de incendio	Proteger equipos y documentación
Protección eléctrica (UPS)	Reducir daños por cortes o variaciones
Inventario de activos	Controlar ubicación y custodia de equipos
Custodia de respaldos	Proteger soportes con información crítica

1.10.1 Clasificación de áreas según criticidad

Una forma práctica de administrar controles físicos es clasificar áreas según su nivel de exposición:

Área	Ejemplo	Control orientativo
Pública	Recepción	Control básico y supervisión
Interna	Oficinas generales	Acceso de personal autorizado
Restringida	Administración, archivo, tesorería	Tarjeta, registro y revisión
Crítica	Sala técnica, centro de datos, bóveda de respaldos	MFA físico, cámara, sensores y auditoría

La intensidad del control debe ser proporcional al impacto. No tiene sentido aplicar el mismo nivel de control a una sala de reuniones y a un espacio donde se conservan respaldos críticos.

1.10.2 Diseño del espacio

La seguridad física debe pensarse desde el diseño del espacio: - Ubicación y circulación de accesos. - Separación entre zonas públicas y privadas. - Identificación de visitantes. - Control de llaves y tarjetas. - Registro de ingresos y egresos. - Protección contra incendios, humedad, temperatura y cortes eléctricos.

1.10.3 Llaves, tarjetas y credenciales

Medio de acceso	Ventaja	Limitación
Llave	Bajo costo y simplicidad	No registra ingresos y puede copiarse
Tarjeta	Revocación rápida y registro	Puede prestarse o perderse

Medio de acceso	Ventaja	Limitación
PIN	Fácil implementación	Puede compartirse u observarse
Credencial móvil	Flexibilidad	Depende del dispositivo
Biometría	Vincula acceso con rasgo personal	Requiere protección de datos biométricos

1.11 Biometría como control físico y lógico

La biometría utiliza características físicas o conductuales para identificar o verificar personas. Puede incluir huella dactilar, rostro, iris, retina, voz, geometría de la mano, firma dinámica, patrones vasculares o comportamiento de uso. Su finalidad es mejorar la validación de identidad y reducir el préstamo de credenciales.

Método biométrico	Ventaja	Limitación
Huella dactilar	Rápida y ampliamente difundida	Puede fallar por cortes, suciedad o desgaste
Reconocimiento facial	Sin contacto y ágil	Sensible a iluminación, ángulo o cambios de apariencia
Iris o retina	Alta precisión	Mayor costo y percepción de invasividad
Voz	Útil en validación remota	Afectada por resfrío, ruido o imitación
Firma dinámica	Vinculada a aprobación documental	Requiere dispositivos específicos y puede variar

Método biométrico	Ventaja	Limitación
Patrón vascular	Difícil de copiar	Requiere sensores especializados
Biometría conductual	Puede operar de modo continuo	Requiere análisis cuidadoso de privacidad

1.11.1 Riesgos administrativos de la biometría

Los datos biométricos son especialmente sensibles: si una contraseña se filtra, puede cambiarse; si se compromete una plantilla biométrica, el problema es mucho más complejo.

Riesgo	Control necesario
Falso rechazo	Procedimiento alternativo seguro
Falsa aceptación	Ajuste de sensibilidad y monitoreo
Suplantación	Detección de vida y detección de presentación
Uso excesivo de datos	Minimización y finalidad definida
Conflictos de privacidad	Comunicación, reglas claras y protección

La biometría no debe adoptarse por moda tecnológica, sino por análisis de riesgo. Exige consentimiento informado, finalidad clara, almacenamiento seguro de plantillas, restricción de acceso, eliminación ante desvinculación y evaluación de impacto en privacidad.

1.11.2 Biometría y autenticación multifactor

La biometría puede integrar un esquema de autenticación multifactor: tarjeta más huella, PIN más rostro, o credencial móvil más reconocimiento facial. No conviene depender de un único factor cuando el área o sistema es crítico.

1.12 Controles de acceso lógico

Los controles de acceso lógico regulan quién puede ingresar a sistemas, datos, redes, aplicaciones y servicios. Se apoyan en tres conceptos básicos:

Concepto	Pregunta que responde	Ejemplo
Identificación	¿Quién dice ser el usuario?	Nombre de usuario
Autenticación	¿Cómo demuestra que es quien dice ser?	Contraseña, token, biometría
Autorización	¿Qué puede hacer una vez autenticado?	Consultar, cargar, aprobar o eliminar
Trazabilidad	¿Qué hizo y cuándo?	Log de auditoría
Baja	¿Cuándo deja de tener acceso?	Revocación por desvinculación

1.12.1 Factores de autenticación

Los factores clásicos de autenticación son:

Factor	Descripción	Ejemplo
Algo que se sabe	Información que el usuario conoce	Contraseña, PIN
Algo que se tiene	Objeto o dispositivo en posesión	Token, tarjeta, celular
Algo que se es	Rasgo biométrico	Huella, rostro, iris, voz

La **autenticación multifactor (MFA)** combina factores de categorías distintas. Contraseña más pregunta secreta no es MFA real, porque ambas pertenecen al mismo factor: conocimiento.

1.12.2 MFA, tokens y passkeys

Mecanismo	Uso	Observación
OTP	Código de un solo uso	Puede generarse por aplicación o dispositivo
TOTP	Código temporal basado en tiempo	Cambia cada pocos segundos
Token físico	Dispositivo de autenticación	Debe registrarse, revocarse y custodiarse
Tarjeta inteligente	Credencial con almacenamiento seguro	Puede combinarse con PIN
Passkey	Clave de acceso sin contraseña	Reduce phishing y reutilización de claves

Las **passkeys** se basan en criptografía de clave pública: el servicio conserva una clave pública y el dispositivo del usuario conserva una clave privada que no se comparte, lo que reduce radicalmente el riesgo de phishing y robo masivo de contraseñas.

1.12.3 Buenas prácticas con contraseñas

Práctica	Finalidad
Contraseñas largas	Reducir adivinación
Prohibición de claves compartidas	Mantener trazabilidad
Bloqueo por intentos fallidos	Reducir ataques de fuerza bruta
Recuperación segura	Evitar apropiación de cuentas
MFA en sistemas críticos	Reducir impacto de contraseña robada
Hash y salt	Proteger contraseñas almacenadas

El cambio periódico de contraseña no debe ser el único control. MFA, longitud adecuada, bloqueo de claves comunes y monitoreo suelen ser más eficaces que rotaciones frecuentes sin criterio.

1.12.4 Revisión del ciclo de vida del usuario

Los permisos no deben asignarse una vez y olvidarse. La organización cambia: las personas ingresan, se desvinculan, cambian de puesto o dejan de necesitar ciertos accesos.

Momento del ciclo	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

Regla de gestión: todo usuario debe tener únicamente los permisos necesarios para cumplir su función, y nada más.

1.13 IAM, SSO, RBAC, ABAC y PAM

La administración moderna de accesos requiere herramientas y criterios de gobierno específicos.

Sigla	Nombre	Explicación
IAM	*Identity and Access Management*	Gestión del ciclo de vida de identidades y accesos
SSO	*Single Sign-On*	Inicio de sesión único para varias aplicaciones
RBAC	*Role-Based Access Control*	Acceso basado en roles
ABAC	*Attribute-Based Access Control*	Acceso basado en atributos o condiciones
PAM	*Privileged Access Management*	Gestión de accesos privilegiados

IAM permite administrar altas, cambios, permisos, revisiones y bajas. El ciclo básico incluye ingreso, movimiento y salida. El movimiento interno es crítico: una persona que cambia de puesto debe perder permisos anteriores y recibir solo los nuevos permisos necesarios.

SSO permite autenticarse una vez y acceder a varias aplicaciones autorizadas. Mejora la experiencia y facilita bajas centralizadas, pero concentra riesgo. Debe combinarse con MFA, monitoreo y políticas de sesión.

RBAC asigna permisos por rol. **ABAC** agrega condiciones: ubicación, horario, dispositivo, monto o tipo de operación.

Modelo	Ventaja	Riesgo
RBAC	Simple y consistente	Roles demasiado amplios
ABAC	Flexible y contextual	Mayor complejidad de administración

Los roles no deben ser genéricos. Un rol llamado “usuario total” suele indicar falta de diseño.

PAM se ocupa de cuentas privilegiadas que pueden administrar sistemas, crear usuarios, modificar configuraciones o cambiar reglas de seguridad.

Control PAM	Finalidad
Cuenta administrativa separada	Evitar uso diario de privilegios
MFA fuerte	Reducir riesgo de compromiso
Bóveda de credenciales	Proteger claves privilegiadas
Registro de sesión	Mantener evidencia de acciones
Acceso temporal (JIT)	Evitar privilegios permanentes
Revisión frecuente	Detectar abusos o accesos innecesarios

1.13.1 Acceso condicional y gestión de sesiones

El acceso condicional evalúa el contexto antes de permitir ingreso o habilitar acciones sensibles:

Situación	Respuesta posible
Acceso desde ubicación inusual	Exigir MFA adicional
Dispositivo no administrado	Limitar acceso o bloquear
Horario fuera de lo habitual	Generar alerta
Descarga masiva de datos	Bloquear o requerir aprobación
Operación financiera sensible	Exigir reautenticación

La expiración de sesiones por inactividad reduce el riesgo de que otra persona use una sesión abandonada. El bloqueo por intentos fallidos reduce ataques de fuerza bruta, pero debe diseñarse con equilibrio para evitar que se use como mecanismo de denegación de servicio.

1.14 Controles de aplicación

Los controles de aplicación se incorporan dentro de los sistemas de negocio. Protegen operaciones, datos, cálculos, formularios, autorizaciones y reportes.

Control de aplicación	Función
Máscara de entrada	Exige formato válido de carga
Campo obligatorio	Evita registros incompletos
Validación de rango	Impide importes o fechas inválidas
Límite por monto	Controla operaciones relevantes
Regla de autorización	Exige aprobación según condición
Formulario prenumerado	Detecta faltantes o duplicados
Total de control	Compara importes o cantidades procesadas
Log de auditoría	Registra operaciones relevantes
Control cruzado	Compara datos entre sistemas o áreas
Dígito verificador	Identifica errores en códigos o números

Ejemplo: si se modifica una cuenta bancaria de proveedor, el sistema debería registrar usuario, fecha, dato anterior, dato nuevo, motivo y aprobación. También debería generar un reporte de cambios para revisión posterior.

1.15 Controles de comunicaciones

Las comunicaciones son esenciales para la operación moderna. La información circula por redes internas, internet, correo electrónico, sistemas en la nube, conexiones remotas y APIs. Los controles de comunicaciones buscan evitar interceptaciones, modificaciones, accesos indebidos o filtraciones durante la transmisión.

Control de comunicaciones	Función
Segmentación de redes y VLANs	Separar áreas o servicios para reducir exposición
Firewalls	Filtrar tráfico permitido y bloqueado
IDS/IPS	Detectar o prevenir intrusiones
VPN	Proteger conexiones remotas
Cifrado de comunicaciones	Proteger datos en tránsito
Filtros antiphishing	Reducir correos fraudulentos
Bloqueo de dominios maliciosos	Evitar navegación riesgosa
DLP en correo y red	Detectar salida indebida de información
Certificados digitales	Proteger autenticidad y cifrado
SIEM	Consolidar eventos y generar alertas
Redundancia de enlaces	Mantener continuidad ante fallas de conectividad
Registro de conexiones	Mantener trazabilidad

1.15.1 Trabajo remoto y comunicaciones seguras

El trabajo remoto amplía la superficie de exposición. Una política de comunicaciones debe contemplar: - Uso obligatorio de VPN cuando corresponda. - Autenticación multifactor. - Dispositivos autorizados y cifrado de discos. - Actualizaciones de seguridad al día. - Prohibición de compartir equipos de trabajo. - Reglas para almacenamiento en la nube. - Procedimientos de reporte ante pérdida o robo de equipos.

1.16 Seguridad de datos

Los datos son uno de los activos más valiosos de cualquier organización. La protección debe pensarse durante **todo el ciclo de vida** del dato.

Etapa	Control posible
Creación o captura	Validaciones y clasificación
Almacenamiento	Cifrado en reposo y permisos de acceso
Uso	Acceso mínimo necesario
Modificación	Registro de auditoría y autorización
Transmisión	Cifrado en tránsito
Archivo	Política de retención documental
Eliminación	Borrado seguro
Recuperación	Backup y restore

1.16.1 Clasificación de la información

No toda la información tiene el mismo valor ni requiere el mismo nivel de protección:

Nivel	Descripción	Ejemplo
Pública	Puede difundirse sin restricciones	Folleto institucional
Interna	Uso dentro de la organización	Procedimientos internos
Confidencial	Acceso limitado a personas autorizadas	Legajos, contratos, datos financieros

Nivel	Descripción	Ejemplo
Crítica / Restringida	Información cuya pérdida detiene procesos o genera daño grave	Datos salariales, claves, información estratégica

La clasificación permite definir quién puede acceder, cómo debe almacenarse, cómo debe transmitirse y cuándo debe eliminarse la información.

1.16.2 Controles principales sobre los datos

Control	Finalidad
Clasificación y etiquetado	Identificar sensibilidad de la información
Cifrado en reposo	Proteger datos almacenados
Cifrado en tránsito	Proteger datos transmitidos
Hashes y firmas digitales	Verificar integridad
DLP (*Data Loss Prevention*)	Prevenir fuga de datos sensibles
Restricción de dispositivos removibles	Reducir riesgo de copia no autorizada o malware
Políticas de retención	Definir cuánto tiempo se conserva la información
Eliminación segura	Evitar recuperación indebida de datos descartados

1.17 Políticas y controles administrativos

Las políticas administrativas son normas internas que regulan la conducta de las personas y el uso de los recursos tecnológicos. Muchos incidentes no se producen por fallas técnicas, sino por errores humanos, ausencia de procedimientos, negligencia, falta de capacitación o indefinición de responsabilidades.

1.17.1 Manual de políticas de seguridad

Toda organización debería contar como mínimo con: - Normas generales de acceso y uso de sistemas. - Política de uso aceptable de internet y correo electrónico. - Procedimiento de alta, baja y modificación de usuarios. - Gestión de contraseñas y uso de MFA. - Tratamiento de información confidencial. - Protocolo ante incidentes de seguridad. - Política de trabajo remoto y BYOD. - Declaración de confidencialidad. - Política de backup y recuperación.

1.17.2 Buenas prácticas administrativas

Práctica	Objetivo
Escritorio limpio	Evitar exposición de documentos sensibles
Bloqueo automático de pantallas	Impedir uso no autorizado de equipos abandonados
Armarios bajo llave	Proteger documentación física
Impresión segura	Evitar que documentos queden expuestos en impresoras
Identificación visible	Diferenciar personal, visitas y terceros
Registro de visitas	Mantener trazabilidad de accesos externos
Acuerdos de confidencialidad	Proteger información frente a empleados y terceros

1.17.3 Capacitación y cultura de seguridad

La capacitación debe ser continua, periódica y diferenciada por rol. Los contenidos mínimos incluyen: - Buenas prácticas de seguridad digital. - Protección de datos personales. - Uso seguro de contraseñas. - Detección de phishing e ingeniería social. - Reporte de incidentes. - Riesgos del trabajo remoto.

Una cultura de seguridad fuerte se construye cuando los usuarios entienden que la seguridad no es responsabilidad exclusiva del área técnica. Es una responsabilidad compartida.

1.17.4 Supervisión de proveedores

Los proveedores también representan riesgos al tener acceso a oficinas, sistemas, datos o infraestructura. Se recomienda: - Firmar acuerdos de confidencialidad. - Incluir cláusulas de seguridad en contratos. - Limitar accesos según necesidad operativa. - Registrar actividades de terceros. - Exigir estándares mínimos de seguridad. - Definir responsabilidades ante incidentes.

1.18 El factor humano e ingeniería social

Aunque existan controles técnicos avanzados, la seguridad sigue dependiendo del comportamiento humano. Las personas pueden cometer errores, compartir claves, caer en engaños o ignorar procedimientos. Con capacitación y cultura adecuada, también pueden transformarse en una **línea de defensa activa**.

1.18.1 Ingeniería social

La ingeniería social consiste en manipular a una persona para que realice una acción insegura o entregue información confidencial.

Técnica	Descripción	Ejemplo
Phishing	Correo fraudulento que simula una entidad confiable	Solicitud falsa de actualización de clave
Vishing	Engaño mediante llamada telefónica	Supuesto soporte técnico pide datos de acceso
Pretexting	Creación de una historia falsa	Encuesta falsa para obtener datos personales

Técnica	Descripción	Ejemplo
Tailgating	Ingreso físico detrás de una persona autorizada	Entrar sin credencial aprovechando una puerta abierta
Spear phishing	Ataque personalizado a una persona específica	Mensaje dirigido al gerente financiero
Fraude del CEO	Suplantación de autoridad interna	Pedido falso de transferencia urgente

1.18.2 Perfilamiento de individuos

Los atacantes pueden recolectar información pública para construir perfiles: redes sociales, sitios web, publicaciones, cargos, contactos o rutinas. Esa información puede utilizarse para crear ataques más creíbles. Por ejemplo, si se sabe que un directivo está de viaje, un atacante puede enviar un mensaje falso solicitando una transferencia urgente en su nombre.

1.18.3 Mitigación del riesgo humano

Medida	Objetivo
Capacitación continua	Mantener al personal alerta
Simulacros de phishing	Medir y mejorar la respuesta
Doble confirmación	Validar solicitudes sensibles por otro canal
Cultura de reporte	Informar incidentes sin temor a sanciones injustas
Políticas claras	Reducir ambigüedades

Medida	Objetivo
Mensajes periódicos de concientización	Reforzar hábitos seguros

1.19 Principios de mínima exposición y mínimos privilegios

Dos principios son fundamentales para reducir riesgos y forman parte de la estrategia de defensa en profundidad.

1.19.1 Mínima exposición

El principio de mínima exposición indica que los sistemas, datos e infraestructuras deben exponerse lo menos posible: solo deben estar visibles, accesibles o publicados los recursos estrictamente necesarios.

Aplicaciones prácticas: - Segmentar redes y usar zonas desmilitarizadas para servicios públicos. - Desactivar servicios innecesarios y cerrar puertos no utilizados. - Restringir consolas administrativas. - Evitar exposición pública de archivos de configuración. - Limitar información visible sobre versiones de software.

1.19.2 Mínimos privilegios

El principio de mínimos privilegios indica que cada usuario, proceso o sistema debe tener únicamente los permisos necesarios para cumplir su función.

Aplicaciones prácticas: - No usar cuentas administrativas para tareas diarias. - Asignar permisos por rol y revocar los innecesarios. - Revisar periódicamente accesos. - Separar funciones operativas, administrativas y de auditoría. - Otorgar permisos temporales cuando sea necesario. - Registrar accesos privilegiados.

Principio	Reduce	Ejemplo
Mínima exposición	Cantidad de puntos vulnerables	No publicar una consola administrativa en internet

Principio	Reduce	Ejemplo
Mínimos privilegios	Impacto si un acceso es comprometido	Un usuario de ventas no puede modificar parámetros contables

1.20 Evaluación, auditoría y mejora continua

La seguridad no puede ser estática. Los controles que hoy resultan adecuados pueden quedar obsoletos por cambios tecnológicos, nuevas amenazas, crecimiento organizacional o modificaciones normativas.

1.20.1 Tipos de auditoría

Tipo de auditoría	Característica	Finalidad
Interna	Realizada por personal de la organización	Revisar cumplimiento y detectar mejoras
Externa	Realizada por especialistas independientes	Aportar objetividad y validar controles
Técnica	Enfocada en infraestructura y seguridad lógica	Detectar vulnerabilidades
Administrativa	Enfocada en políticas y procedimientos	Verificar control interno
Normativa	Enfocada en cumplimiento legal o estándares	Evaluar cumplimiento regulatorio

1.20.2 Mejora continua — Ciclo PDCA

Etapa	Significado	Aplicación en seguridad
Planificar	Definir objetivos y controles	Diseñar políticas y matriz de riesgos
Hacer	Implementar medidas	Activar controles y capacitar usuarios
Verificar	Evaluar resultados	Auditar, medir incidentes y revisar logs
Actuar	Corregir y mejorar	Actualizar políticas y reforzar controles

1.20.3 Indicadores de eficacia de controles

Indicador	Qué permite observar
Porcentaje de accesos revisados	Cumplimiento de revisión periódica
Tiempo promedio de baja de usuarios	Rapidez para cerrar accesos
Cantidad de usuarios con privilegios excesivos	Riesgo de permisos innecesarios
Cantidad de cambios sin aprobación	Debilidad en gestión de cambios
Porcentaje de backups restaurados exitosamente	Capacidad real de recuperación
Tiempo promedio de recuperación	Eficacia recuperatoria
Cantidad de incidentes detectados por monitoreo	Funcionamiento de controles detectivos
Cantidad de conciliaciones pendientes	Debilidad de control financiero

Indicador	Qué permite observar
Excepciones vencidas	Riesgo de permisos temporales no cerrados

1.21 Guía práctica de implementación

Hoja de ruta para implementar controles de seguridad en una organización de tamaño mediano (referencia: 150 empleados, una sede central y dos regionales, red interna, servidores locales y nube).

1.21.1 Etapa 1: diagnóstico y planificación

- Relevar infraestructura física y lógica.
- Identificar activos críticos y revisar accesos actuales.
- Evaluar nivel de conciencia del personal.
- Designar un responsable de seguridad.
- Elaborar una matriz inicial de riesgos.

1.21.2 Etapa 2: controles físicos

- Tarjetas de proximidad para oficinas y sala de servidores con cerradura biométrica.
- Registro digital de ingresos y egresos.
- Cámaras de videovigilancia, sensores de temperatura y humo.
- Política de escritorio limpio y bloqueo automático de equipos.

1.21.3 Etapa 3: controles lógicos y protección de datos

- Activar MFA en sistemas críticos.
- Segmentar la red por áreas y aplicar mínimos privilegios.

- Cifrar datos en tránsito y en reposo.
- Implementar política robusta de contraseñas y revisión periódica de permisos.

1.21.4 Etapa 4: controles administrativos

- Política de seguridad de la información y uso aceptable de TI.
- Política de trabajo remoto y BYOD.
- Acuerdos de confidencialidad.
- Procedimiento de alta, baja y modificación de usuarios.
- Revisión trimestral de permisos.

1.21.5 Etapa 5: capacitación y concientización

- Capacitación semestral obligatoria.
- Boletines mensuales de seguridad.
- Simulacros de phishing y de fuga de datos.
- Entrenamiento específico por rol.

1.21.6 Etapa 6: auditoría, monitoreo y mejora continua

- Activar monitoreo de logs e implementar SIEM si el tamaño lo justifica.
- Revisar accesos y privilegios cada seis meses.
- Auditar backups mensualmente.
- Auditoría interna semestral y auditoría externa anual.
- Actualizar el plan de seguridad cada doce meses.

1.21.7 Matriz resumida de acciones

Área	Acción	Responsable sugerido	Frecuencia
Seguridad física	Instalar CCTV, control de accesos y biometría	TI / Infraestructura	Inicial y revisión anual
Seguridad lógica	Activar MFA, RBAC y revisión de permisos	TI	Permanente
Administración	Redactar y actualizar políticas	Comité de seguridad	Anual
Capacitación	Realizar cursos y simulacros	RR.HH. / Seguridad	Semestral
Auditoría	Ejecutar auditoría interna	Auditor interno	Cada 6 meses
Backups	Revisar copias y realizar pruebas de restauración	Responsable de TI	Mensual
Proveedores	Revisar accesos y contratos	Compras / Legal / Seguridad	Anual
Incidentes	Probar protocolo de respuesta	Seguridad / TI	Anual

1.22 Ejemplo integrador: pago a proveedores

El proceso de pago a proveedores permite observar cómo interactúan distintos controles en una operación administrativa crítica.

Etapa	Control	Tipo
Alta de proveedor	Validación documental y aprobación	Preventivo
Carga de cuenta bancaria	Doble aprobación y confirmación por canal independiente	Preventivo
Generación de pago	Límite por monto y separación de funciones	Preventivo
Aprobación	Usuario autorizado con MFA	Preventivo
Ejecución	Registro de operación y trazabilidad	Preventivo / Detectivo
Detección	Reporte de pagos inusuales y conciliación bancaria	Detectivo
Corrección	Reversión o ajuste documentado	Correctivo
Recuperación	Restauración de información si falla el sistema	Recuperatorio
Auditoría	Revisión de cambios, aprobaciones y evidencias	Detectivo

Este ejemplo muestra que un proceso administrativo crítico no se protege con un único control. Requiere diseño preventivo, detección oportuna, corrección documentada y capacidad de recuperación.

1.23 Ideas clave

- La seguridad de la información requiere un enfoque integral: combinar controles físicos, lógicos, administrativos y culturales.
- Todo control debe tener **objetivo, responsable, procedimiento, evidencia y revisión**. Sin estos cinco elementos, el control es difícil de auditar y sostener.
- Los **controles preventivos** son la primera línea de defensa y buscan evitar incidentes antes de que ocurran, pero ningún control preventivo es suficiente por sí solo.
- Los **controles detectivos** dan visibilidad: permiten saber que algo ocurrió y brindan evidencia para investigarlo. Su valor depende de la oportunidad de detección.
- Los **controles correctivos** deben atacar la causa del problema, no solo el síntoma. Toda corrección de datos sensibles debe quedar documentada con trazabilidad.
- Los **controles recuperatorios** reducen el impacto de un incidente. Un backup sin prueba de restauración no es evidencia suficiente de capacidad de recuperación.
- La **tríada CIA** — confidencialidad, integridad y disponibilidad — organiza los objetivos de protección de cualquier sistema de información.
- Los controles físicos son tan importantes como los lógicos: un sistema puede tener contraseñas robustas y seguir siendo vulnerable si la sala técnica está sin protección.
- **MFA, IAM, RBAC, ABAC y PAM** fortalecen la gestión moderna de accesos y permiten asignar, controlar y revocar permisos de manera ordenada.
- Las **passkeys** y los tokens reducen la dependencia de contraseñas y el riesgo de phishing.

- El principio de **mínima exposición** reduce la cantidad de puntos vulnerables. El de **mínimos privilegios** reduce el impacto si un acceso es comprometido.
- El factor humano puede ser la debilidad más importante o la primera línea de defensa, según la capacitación y la cultura organizacional.
- La **ingeniería social** aprovecha confianza, urgencia y desconocimiento. La doble confirmación y los simulacros son contramedidas clave.
- La **mejora continua** es indispensable porque las amenazas cambian. Los controles deben evaluarse, auditarse y actualizarse de manera periódica.
- La seguridad debe entenderse como una función de gestión. Su objetivo no es únicamente proteger computadoras, sino preservar procesos, información, responsabilidades, continuidad operativa y confianza institucional.

1.24 Preguntas de evaluación

1. ¿Por qué la seguridad de la información no puede depender de un único control?
2. ¿Qué significan los tres principios de la tríada CIA? Proporcione un ejemplo organizacional para cada uno.
3. ¿Qué cinco elementos debe tener un control para ser útil como herramienta de gestión? Ilustre con un ejemplo concreto.
4. ¿Cuál es la diferencia entre un control preventivo, uno detectivo, uno correctivo y uno recuperatorio?
5. ¿Qué ejemplos de controles preventivos pueden aplicarse en un proceso de pagos a proveedores?
6. ¿Qué función cumplen los logs y las pistas de auditoría? ¿Por qué un registro que nadie revisa tiene valor limitado?
7. ¿Por qué las conciliaciones son controles detectivos relevantes? Proporcione un ejemplo aplicado a contabilidad o pagos.

8. ¿Por qué una acción correctiva debe buscar la causa del problema y no solo corregir el síntoma?
9. ¿Qué condiciones deben cumplirse para que una corrección de datos sensibles sea aceptable desde el punto de vista del control interno?
10. ¿Cuál es la diferencia entre backup y restore? ¿Por qué el backup debe probarse periódicamente?
11. ¿Qué significan RTO y RPO? ¿Cómo se relacionan con la elección de la frecuencia de backup?
12. ¿Qué activos protegen los controles físicos? ¿Por qué son tan importantes como los controles lógicos?
13. ¿Cómo debe clasificarse un espacio de trabajo según su criticidad para definir controles físicos?
14. ¿Qué diferencia existe entre identificación, autenticación y autorización?
15. ¿Qué es MFA y por qué fortalece el control de acceso? ¿Qué significa que contraseña más pregunta secreta no es MFA real?
16. ¿Qué son las passkeys y qué riesgos reducen respecto de las contraseñas tradicionales?
17. ¿Qué diferencia existe entre RBAC y ABAC? ¿Por qué los roles no deben ser genéricos?
18. ¿Por qué las cuentas privilegiadas requieren controles especiales? ¿Qué medidas recomienda PAM?
19. ¿Qué ventajas y riesgos presentan los controles biométricos? ¿Por qué no deben adoptarse por moda tecnológica?
20. ¿Qué controles de aplicación pueden reducir errores en sistemas administrativos?

21. ¿Qué significa el principio de mínima exposición? ¿Y el de mínimos privilegios?
22. ¿Por qué la ingeniería social es un riesgo relevante para las organizaciones? ¿Qué técnicas utiliza y cómo pueden mitigarse?
23. ¿Por qué los proveedores externos representan un riesgo de seguridad? ¿Qué controles deben exigirse?
24. ¿Qué es el ciclo PDCA y cómo se aplica a la mejora continua de los controles de seguridad?
25. ¿Qué indicadores pueden usarse para evaluar la eficacia de los controles de seguridad?
26. ¿Cómo se integran controles preventivos, detectivos, correctivos y recuperatorios en el proceso de pago a proveedores?
27. ¿Por qué la cultura organizacional puede considerarse un control de seguridad transversal?

1.25 Glosario

Término o sigla	Explicación
ABAC (*Attribute-Based Access Control*)	Control de acceso basado en atributos. Asigna permisos según condiciones como ubicación, horario, dispositivo, monto o tipo de dato.
Autenticación (*authentication*)	Proceso que verifica que una identidad declarada corresponde a quien intenta acceder.
Autorización (*authorization*)	Definición de lo que un usuario puede hacer dentro de un sistema luego de autenticarse.

Término o sigla	Explicación
Backup	Copia de respaldo destinada a recuperar información ante pérdida, daño o interrupción. Solo tiene valor real si la restauración fue probada.
BCP (*Business Continuity Plan*)	Plan de continuidad del negocio. Define cómo sostener funciones críticas ante interrupciones.
BIA (*Business Impact Analysis*)	Análisis de impacto en el negocio. Permite identificar procesos críticos y prioridades de recuperación.
Biometría (*biometrics*)	Identificación o verificación basada en características físicas o conductuales de una persona.
CASB (*Cloud Access Security Broker*)	Intermediario de seguridad de acceso a la nube. Ayuda a controlar el uso de servicios cloud.
CCTV	*Closed-Circuit Television*. Sistema de videovigilancia mediante cámaras.
CIA	*Confidentiality, Integrity, Availability*. Confidencialidad, integridad y disponibilidad. Tríada básica de la seguridad de la información.
Control correctivo	Medida que corrige una falla, error, desvío o vulnerabilidad detectada, atacando el síntoma y la causa.

Término o sigla	Explicación
Control detectivo	Medida que permite identificar eventos, errores o irregularidades que ya ocurrieron o están ocurriendo.
Control preventivo	Medida que busca evitar que ocurra un incidente, error o irregularidad, actuando antes del evento.
Control recuperatorio	Medida que permite restaurar información, sistemas o procesos luego de una interrupción.
Defense in depth	Defensa en capas. Estrategia que combina varios controles para reducir, detectar, corregir y recuperar ante incidentes.
DLP (*Data Loss Prevention*)	Prevención de pérdida de datos. Controles destinados a evitar salidas no autorizadas de información.
DRP (*Disaster Recovery Plan*)	Plan de recuperación ante desastres. Define cómo recuperar infraestructura y sistemas tecnológicos.
Firewall	Cortafuegos. Control que filtra tráfico de red permitido o bloqueado.
Hash	Función que transforma un dato en una huella digital no reversible. Se usa para proteger contraseñas almacenadas.

Término o sigla	Explicación
IAM (*Identity and Access Management*)	Gestión de identidades y accesos. Administra altas, permisos, revisiones, cambios y bajas de usuarios.
IDS / IPS (*Intrusion Detection / Prevention System*)	Sistema de detección o prevención de intrusiones. Analiza actividad para identificar y bloquear patrones sospechosos.
Identificación (*identification*)	Declaración de identidad de un usuario, por ejemplo mediante nombre de usuario o legajo.
Ingeniería social (*social engineering*)	Técnica de manipulación para que una persona realice una acción insegura o entregue información confidencial.
JEA (*Just-Enough Access*)	Acceso solo suficiente. Permisos mínimos necesarios para una tarea concreta.
JIT (*Just-In-Time*)	Acceso justo a tiempo. Habilitación temporal de permisos solo durante el período necesario.
Least privilege	Principio de mínimo privilegio. Cada usuario debe tener solo los permisos necesarios para cumplir su función.
Log	Registro automático de actividad de sistemas, usuarios o dispositivos.

Término o sigla	Explicación
MFA (*Multi-Factor Authentication*)	Autenticación multifactor. Método que exige dos o más factores de autenticación de categorías distintas.
Offboarding	Proceso formal de desvinculación que incluye baja de accesos, devolución de equipos y cierre de credenciales.
OTP (*One-Time Password*)	Contraseña de un solo uso. Código que se utiliza una vez para autenticar.
PAM (*Privileged Access Management*)	Gestión de accesos privilegiados. Control específico sobre cuentas con permisos elevados.
Passkey	Clave de acceso sin contraseña basada en criptografía de clave pública. Reduce phishing y reutilización de claves.
PDCA	Ciclo de mejora continua: Planificar (*Plan*), Hacer (*Do*), Verificar (*Check*), Actuar (*Act*).
Phishing	Técnica de engaño mediante correos, mensajes o sitios falsos para obtener credenciales u otra información sensible.
PIN (*Personal Identification Number*)	Número personal de identificación.
Pista de auditoría (*audit trail*)	Registro que permite reconstruir qué operación se realizó, quién la ejecutó, cuándo y sobre qué dato.

Término o sigla	Explicación
RBAC (*Role-Based Access Control*)	Control de acceso basado en roles. Asigna permisos según función o cargo.
Restore	Restauración de datos o sistemas desde una copia de respaldo.
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.
Salt	Valor aleatorio agregado al procesamiento de contraseñas para dificultar ataques masivos contra hashes.
Segregación de funciones (*Segregation of Duties, SoD*)	Principio de control interno que evita que una misma persona concentre todas las etapas críticas de un proceso.
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.

Término o sigla	Explicación
SSO (*Single Sign-On*)	Inicio de sesión único. Permite autenticarse una vez y acceder a varias aplicaciones autorizadas.
TOTP (*Time-Based One-Time Password*)	Contraseña de un solo uso basada en tiempo. Cambia cada pocos segundos.
UPS (*Uninterruptible Power Supply*)	Sistema de alimentación ininterrumpida. Mantiene energía ante cortes o variaciones eléctricas.
VLAN (*Virtual Local Area Network*)	Red de área local virtual. División lógica de la red para separar tráfico y reducir exposición.
VPN (*Virtual Private Network*)	Red privada virtual. Canal seguro para acceso remoto a recursos internos.
Spear phishing	Variante de phishing personalizada y dirigida a una persona, cargo u organización específica.
Vishing	Ingeniería social realizada mediante llamada telefónica para obtener información o acceso.