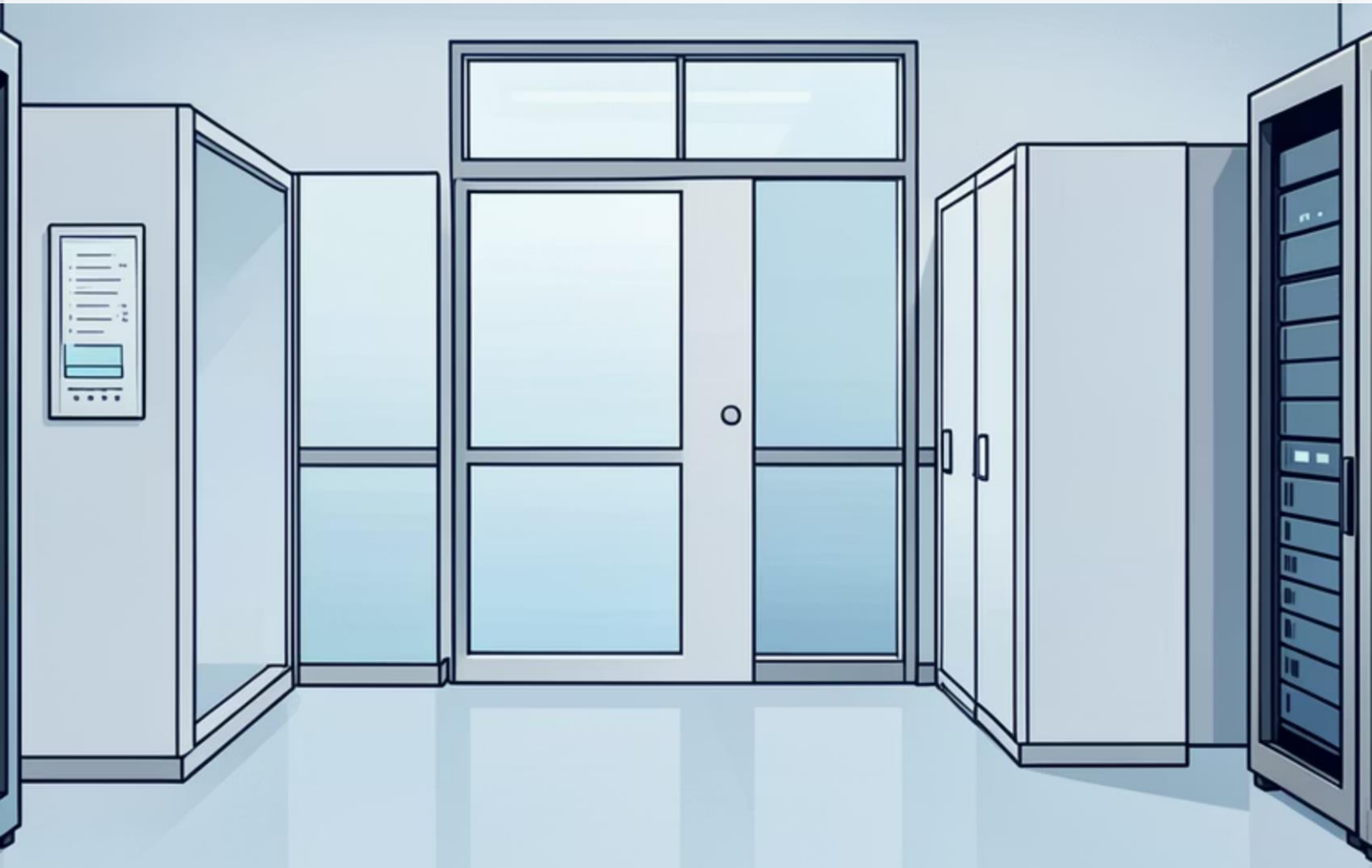
Auditoría IT: Controles clave y evidencias mínimas

Estructura sugerida para documentar y sostener prácticas repetibles

> Sin evidencia, el control no existe. Con evidencia mínima, se sostiene.



Mimetic Advisory

¿Qué es evidencia mínima y por qué sirve?

La evidencia mínima es el registro justo y suficiente que demuestra que un control existe y funciona, sin caer en burocracia paralizante. Es el equilibrio entre auditoría efectiva y operación ágil.

Reduce improvisación

Documentación clara que elimina decisiones arbitrarias

Facilita delegar

Procesos replicables sin depender de memoria institucional

Soporta auditorías

Evidencia lista para presentar a auditores internos o externos

Acelera respuesta

Información disponible para resolver incidentes rápidamente

Control 1: Inventario y criticidad

Qué controlar

Activos y sistemas críticos con dueño asignado

Evidencia mínima

Planilla de activos con clasificación y responsable identificado

Frecuencia

Trimestral o por cambios relevantes

Responsable sugerido

TI + dueño de negocio

A

Impacto

Alto: base de todos los controles

M

Esfuerzo

Medio: requiere coordinación inicial

Sin inventario actualizado, no sabés qué proteger ni a quién consultar cuando algo falla.

Control 2: Accesos (altas/bajas/revisión)

Qué controlar

Altas, bajas y revisiones periódicas de usuarios con privilegios

Evidencia mínima

Registro de altas/bajas + revisión trimestral firmada + administradores separados de usuarios comunes

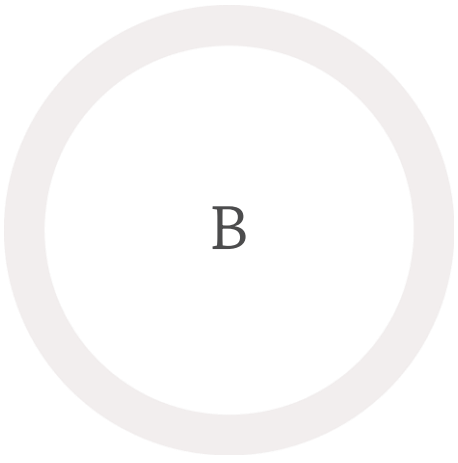
Frecuencia

Continuo para altas/bajas + revisión trimestral de permisos activos

Responsable sugerido

TI + RRHH/Administración

Impacto



Esfuerzo

La mayoría de los incidentes de seguridad provienen de accesos mal gestionados: ex empleados con usuarios activos o permisos excesivos nunca revisados.

Control 3: Cambios (aprobación y trazabilidad)

01

Qué controlar

Cambios en infraestructura, aplicaciones y configuraciones críticas

02

Evidencia mínima

Ticket o mail de aprobación + bitácora de cambios + ventana de mantenimiento documentada

03

Frecuencia

Por cada cambio + revisión mensual de cambios realizados

04

Responsable sugerido

TI/Infraestructura con aprobación de líder técnico

A	M
Impacto	Esfuerzo

Errores típicos

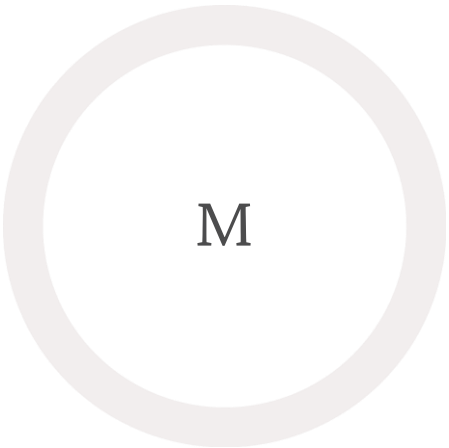
- Cambios de emergencia sin registro posterior
- Aprobaciones verbales sin trazabilidad
- Bitácoras incompletas o desactualizadas

Control 4: Parches y EOL

Mantener sistemas actualizados y gestionar el fin de vida de tecnologías críticas es fundamental para reducir vulnerabilidades conocidas.

Qué controlar	Evidencia mínima	Frecuencia	Responsable sugerido
Parches de seguridad críticos y sistemas en fin de vida (EOL)	Reporte mensual de parches aplicados + lista de sistemas EOL + plan de remediación con dueño y fecha	Mensual para parches críticos, trimestral para revisión de EOL	TI/Infraestructura con escalamiento a Gerencia para EOL

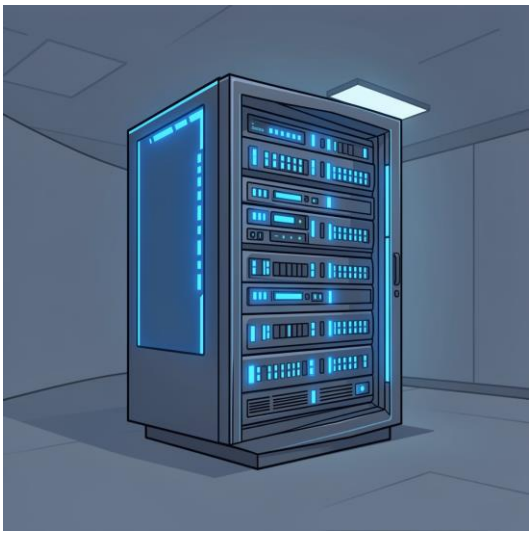
Impacto



Esfuerzo

Los sistemas sin parches son la puerta de entrada más común para ransomware y ataques dirigidos.

Control 5: Backups y restore



Qué controlar

Respaldos de información crítica y capacidad real de recuperación

Evidencia mínima

Logs de backup exitoso + prueba de restore documentada (captura o acta breve) + ubicación de copias offsite

Frecuencia

Diaria/semanal para backups + mensual para pruebas de restore

Responsable sugerido

TI con validación de dueño de negocio en pruebas

A

Impacto

B

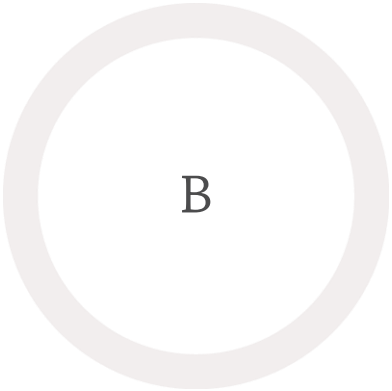
Esfuerzo

> Un backup que nunca se probó no es un backup, es esperanza.

Control 6: Incidentes (registro + lecciones aprendidas)

1	Qué controlar Incidentes de TI, seguridad y operaciones con análisis de causa raíz
2	Evidencia mínima Planilla o tickets de incidentes + cierre con causa identificada y acción correctiva
3	Frecuencia Por cada evento + reporte mensual consolidado
4	Responsable sugerido TI/Operaciones con revisión de Gerencia

Impacto



Esfuerzo

Los incidentes no documentados se repiten. Registrar y aprender de cada evento convierte problemas en mejoras continuas.

Control 7: Proveedores y terceros

La gestión de accesos de terceros es un riesgo crítico frecuentemente subestimado. Proveedores con accesos sin caducidad o sin revisión son vectores comunes de incidentes.

Qué controlar	Evidencia mínima	Frecuencia	Responsable sugerido
Terceros con acceso a sistemas, datos o infraestructura crítica	Lista de terceros activos + accesos con fecha de caducidad + revisión semestral + condiciones mínimas por mail o contrato	Por cada alta de proveedor + revisión semestral de vigentes	TI + Compras/Administración

A	M
Impacto	Esfuerzo

Muchas brechas de seguridad provienen de proveedores con accesos permanentes que ya no trabajan con la empresa.

Tu hoja de ruta: de cero a controles sostenibles

Plantilla sugerida

Excel o Drive con columnas: Control | Evidencia | Frecuencia | Responsable | Estado | Última revisión | Próxima | Hallazgos | Acción

Quick-wins en 7 días

Inventario básico de sistemas críticos, lista de usuarios admin activos, verificación de logs de backup, registro simple de incidentes

1

30 días

Implementar controles de accesos y cambios con evidencia básica

2

60 días

Agregar parches, backups y pruebas de restore documentadas

3

90 días

Completar con proveedores, incidentes y primera revisión integral

---

¿Querés implementar esto en tu empresa?

Armamos tu set de controles y evidencias mínimas adaptado a tu operación: diagnóstico inicial + tablero de seguimiento + capacitación de equipo.

Contactano | Ver más recurso

Formulario web o LinkedIn para coordinar una sesión de diagnóstico sin costo.