Infraestructura: Controles clave y evidencias mínimas

Estructura sugerida para documentar y sostener prácticas repetibles

"Sin evidencia, el control se olvida. Con evidencia mínima, se sostiene."

Mimetic Advisory

¿Qué es evidencia mínima?

La evidencia mínima no es burocracia: es el registro justo y necesario para sostener un control en el tiempo, sin depender de la memoria de una persona.

Baja la improvisación

Cada control tiene un proceso claro y documentado

Permite delegar

Cualquier persona puede ejecutar el control siguiendo la evidencia

Acelera respuestas

En incidentes o auditorías, tenés todo a mano

Evita memoria tribal

La organización no depende de una sola persona

Mimetic Advisory

Control 1: Inventario + Dueños

Qué controlar

Inventario mínimo de activos + criticidad + dueño por servicio

Evidencia mínima

Planilla actualizada + diagrama simple de servicios críticos

Frecuencia

Mensual + por cada alta o baja de equipamiento

Responsable sugerido

TI/Infraestructura

Impacto

ALTO: Sin inventario, no hay gestión posible

Esfuerzo

BAJO: Armado inicial 2-4 hs, mantenimiento 30 min/mes

Control 2: Perímetro y Acceso Remoto

Qué controlar

Reglas mínimas de firewall + acceso remoto controlado (VPN/escritorios remotos)

Evidencia mínima

Snapshot o export de reglas + lista de accesos remotos autorizados

Frecuencia

Mensual + por cada cambio de regla

Responsable sugerido

Infraestructura

Impacto

ALTO: Es la primera línea de defensa

Esfuerzo

BAJO: 15-30 min por revisión

Errores típicos

- Reglas "abiertas" sin revisión hace años
- Accesos remotos sin registro de usuarios activos
- Sin proceso para dar de baja accesos al desvincularse personal

Control 3: Segmentación y Wi-Fi

Qué controlar

Separación mínima de redes: interna / invitados / IoT (impresoras, cámaras, sensores)

Evidencia mínima

Diagrama de VLANs/SSIDs + configuración resumida (1 página)

Frecuencia

Trimestral + por cada cambio de red

Responsable sugerido

Infraestructura

Impacto

MEDIO-ALTO: Limita la propagación de incidentes

Esfuerzo

MEDIO: Setup inicial 4-8 hs, mantenimiento mínimo

Control 4: Backups y Restore

Qué controlar

Backup automatizado + restore probado + copia offline/inmutable cuando aplique

Evidencia mínima

Logs OK de backups + evidencia de restore probado (captura + acta breve)

Frecuencia

Diario/semanal (backup) + mensual (prueba de restore)

Responsable sugerido

Infraestructura

Impacto

CRÍTICO: Sin backup probado, no hay continuidad

Esfuerzo

BAJO-MEDIO: Automatizado + 1-2 hs/mes para pruebas

> **Regla 3-2-1:** 3 copias, 2 medios diferentes, 1 offsite

Control 5: Parches y Ciclos de Vida (EOL)

Qué controlar

Parcheo regular de sistemas operativos y aplicaciones críticas + identificación de equipos EOL

Evidencia mínima

Reporte mensual de parches aplicados + lista de equipos/software EOL + plan de actualización

Frecuencia

Mensual (parcheo) + trimestral (revisión EOL)

Responsable sugerido

Infraestructura

Impacto

ALTO: Previene vulnerabilidades conocidas

Esfuerzo

MEDIO: 2-4 hs/mes + planificación de upgrades

Control 6: Monitoreo Mínimo y Capacidad

Qué controlar

Alertas de caída de servicios, disco lleno, CPU alta, backup fallido, enlaces, accesos remotos sospechosos

Evidencia mínima

Tablero simple de monitoreo + reporte mensual "OK/Issues"

Frecuencia

Continuo (alertas) + mensual (reporte consolidado)

Responsable sugerido

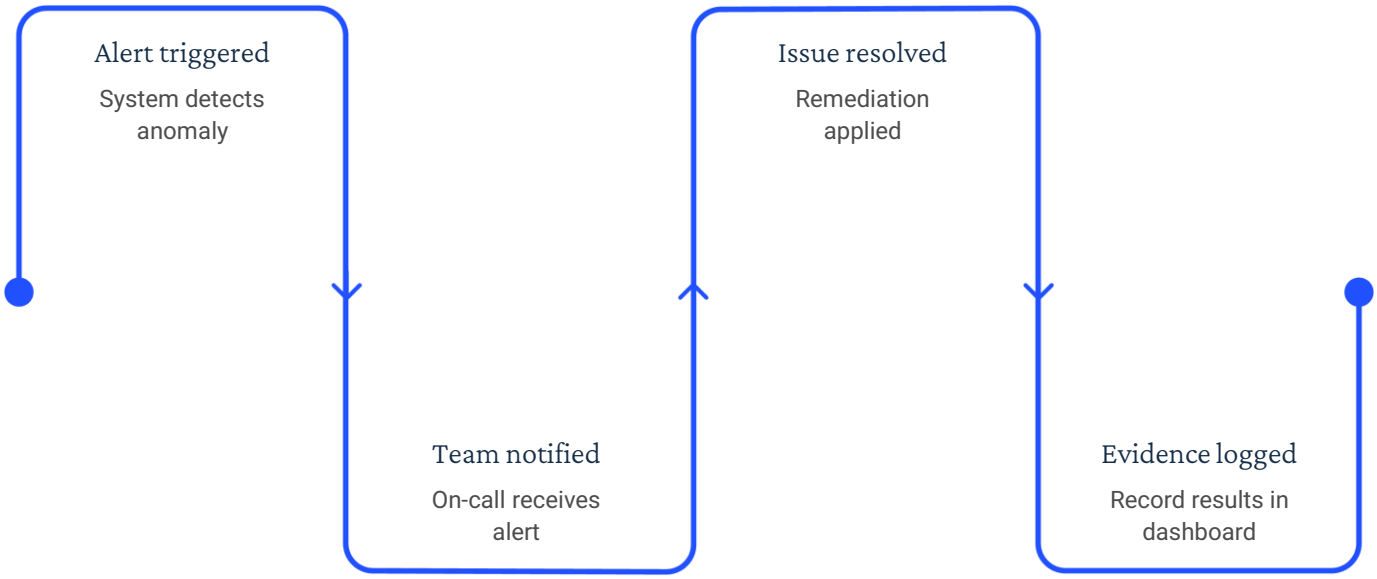
Infraestructura / Operaciones

Impacto

ALTO: Detecta problemas antes de que escalen

Esfuerzo

BAJO: Setup inicial + revisión 1 h/mes



Un buen monitoreo no necesita ser complejo: necesita ser confiable y accionable.

Control 7: Cambios y Configuración

Qué controlar

Cambios aprobados + plan de rollback básico + backup de configuración

Evidencia mínima

Tickets o bitácora de cambios + backup de config antes/después

Frecuencia

Por cada cambio + revisión mensual de bitácora

Responsable sugerido

Infraestructura

Impacto

MEDIO-ALTO: Reduce errores y acelera rollback

Esfuerzo

BAJO: 10-15 min por cambio

> Un cambio sin evidencia es un riesgo sin control

Plantilla + Quick-wins + Roadmap

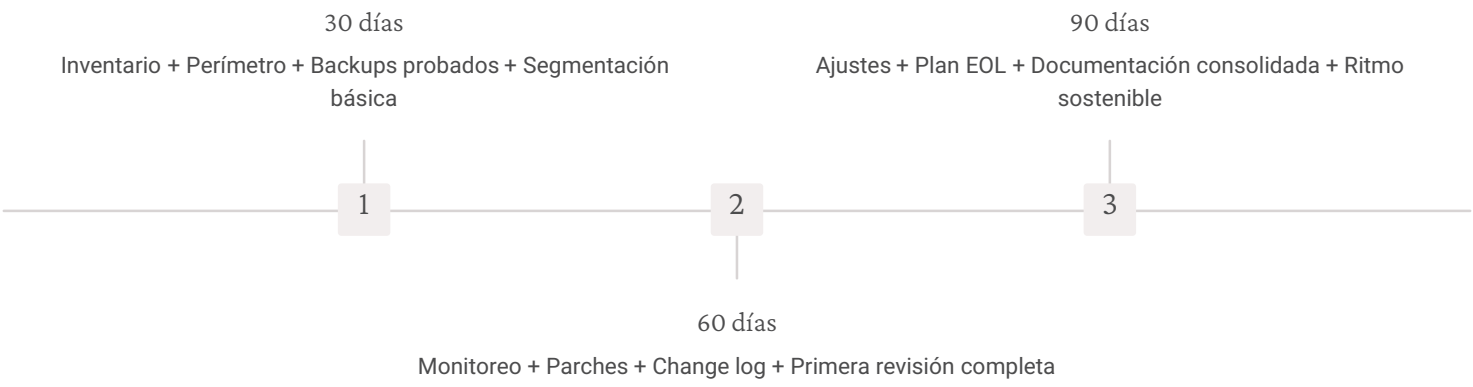
Plantilla sugerida (Excel/Drive)

Control	Evidencia mínima	Frecuencia	Responsable	Estado	Última ejecución	Próxima	Hallazgos
Inventario	Planilla + diagrama	Mensual	TI	—	—	—	—
Perímetro	Snapshot reglas	Mensual	Infra	—	—	—	—

Quick-wins en 7 días

- Armá el inventario básico de servidores y servicios críticos
- Tomá un snapshot de reglas de firewall actuales
- Separá la red Wi-Fi de invitados de la interna
- Probá un restore de backup (aunque sea un archivo)
- Configurá 3 alertas básicas: disco, backup, caída de servicio
- Armá un calendario de parches para el próximo mes
- Creá una bitácora simple para registrar cambios
- Identificá equipos/software EOL en tu inventario

Roadmap sugerido



¿Querés que armemos tu set de controles y tablero de seguimiento adaptado a tu realidad?

Hablemos. Sin humo, solo controles que funcionen.

Contacto

Consultá cómo implementar estos controles en tu organización

Mimetic Advisory