Ciberseguridad: Controles y evidencias mínimas

Estructura sugerida para documentar y sostener prácticas repetibles

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

Diagnósticos de seguridad para PyMEs — **Mimetic Advisory**

Mimetic Advisory

¿Qué es "evidencia mínima"?

El registro más simple que prueba que se hizo

No hace falta documentación perfecta. Hace falta **suficiente** para sostener el control y poder demostrarlo cuando importa: en una auditoría, un incidente o al delegar.

Reduce improvisación

Permite delegar

Acelera auditorías

Baja riesgo de olvidos

La evidencia mínima es tu mejor defensa contra el caos operativo. No es burocracia: es memoria institucional que protege a tu empresa y a tu equipo.

Control 1: Identidades y accesos

Qué control	Evidencia mínima	Frecuencia	Responsable sugerido
MFA en accesos críticos + cuentas admin separadas + revisión periódica de permisos	Listado de cuentas con MFA activo + registro de altas/bajas + revisión trimestral firmada	Por evento (alta/baja) + revisión trimestral completa	TI (implementación) + RRHH/Administración (proceso)

Impacto: ALTO — Protege contra accesos no autorizados

Esfuerzo: MEDIO — Setup inicial + disciplina continua

Control 2: Perímetro y acceso remoto

Qué control	Evidencia mínima
Servicios expuestos mínimos + reglas de firewall revisadas + acceso remoto endurecido	Snapshot de configuración firewall + lista de accesos remotos autorizados + revisión mensual de puertos/reglas
Frecuencia	**Responsable sugerido**
Mensual (revisión) + por cada cambio significativo	TI / Infraestructura

Impacto: ALTO — Primera línea de defensa

Esfuerzo: BAJO — Una vez configurado, mantenimiento mínimo

Errores típicos

- Puerto 3389 abierto a Internet
- Reglas "temporales" que nunca se sacan
- Accesos remotos sin MFA

Control 3: Endpoints (PCs/Notebooks)

Qué control

Protección activa en todos los equipos + hardening básico (firewall, updates) + cifrado en equipos críticos

Evidencia mínima

Reporte mensual de estado (actualizaciones/definiciones) + política de bloqueo activa + muestra de equipos críticos cifrados

Frecuencia

Reporte mensual + verificación continua automática

Responsable sugerido

TI / Soporte técnico

Impacto: ALTO — Los endpoints son el vector de ataque más común

Esfuerzo: MEDIO — Requiere herramienta centralizada y seguimiento

Control 4: Parches y vulnerabilidades

Qué control

Parcheo regular de sistemas + identificación de activos EOL (end of life) + remediación priorizada por criticidad

Evidencia mínima

Reporte mensual de parches aplicados + listado de activos EOL con plan + planilla de vulnerabilidades (dueño/fecha límite)

Frecuencia

Mensual (parches) + trimestral (revisión general)

Responsable sugerido

TI / Seguridad (si existe el rol)

Impacto: ALTO — Vulnerabilidades conocidas son puertas abiertas

Esfuerzo: MEDIO — Requiere disciplina y coordinación con usuarios

Control 5: Backups y restore

La defensa más efectiva contra ransomware es tener copias que el atacante no pueda tocar.

Qué control	Evidencia mínima	Frecuencia	Responsable sugerido
Estrategia 3-2-1: **3 copias, 2 medios diferentes, 1 offsite/offline** + restore probado regularmente	Logs de backup exitosos + evidencia de restore (captura + acta breve) + ubicación documentada de copias	Backup: diario/semanal según criticidad | Restore: mensual (prueba real)	TI / Infraestructura

Impacto: CRÍTICO — Sin backup funcional, un ransomware puede destruir la empresa

Esfuerzo: MEDIO — Setup inicial + verificación mensual

Control 6: Incidentes, logs y monitoreo

Por qué importa

Si no registrás los incidentes, no podés aprender de ellos. Si no guardás logs, no podés investigar cuando algo sale mal.

Qué control

Canal de reporte claro + registro de incidentes + alertas mínimas configuradas + retención de logs críticos

Evidencia mínima

Planilla o tickets de incidentes registrados + reporte mensual de eventos + configuración de retención (muestra de logs)

Frecuencia

Continuo (reporte) + mensual (revisión y métricas)

Responsable sugerido

TI / Operaciones / Mesa de ayuda

Impacto: ALTO — Esencial para investigación y mejora continua

Esfuerzo: BAJO-MEDIO — Requiere proceso, no necesariamente tecnología cara

Control 7: Proveedores y terceros

Los accesos de terceros son una puerta trasera frecuente. Hay que gestionarlos con el mismo rigor que los accesos internos.

Qué control

Terceros identificados + accesos con MFA obligatorio + permisos mínimos necesarios + caducidad automática

Evidencia mínima

Listado actualizado de terceros con acceso + revisión semestral firmada + registro de accesos temporales con fecha de vencimiento

Frecuencia

Por alta/modificación + revisión semestral completa

Responsable

TI + Compras/Administración (según contrato)

Impacto: MEDIO-ALTO — Muchos incidentes vienen por terceros comprometidos

Esfuerzo: BAJO — Más proceso que tecnología

Plantilla + Quick-wins + Roadmap

Plantilla sugerida (Excel/Drive)

Columnas: Control | Evidencia mínima | Frecuencia | Responsable | Estado | Última ejecución | Próxima | Hallazgos | Acción pendiente

Quick-wins en 7 días

- Activar MFA en correo corporativo
- Separar cuentas admin de uso diario
- Inventario mínimo de activos críticos
- Cerrar puertos/servicios innecesarios
- Hacer una prueba de restore real

30 días: Base

MFA, backups + restore probado, reducir exposición, inventario crítico

- Listar terceros con acceso activo
- Aplicar parches críticos pendientes
- Bloquear macros y scripts no firmados
- Crear canal claro de reporte de incidentes
- Revisar reglas de firewall obsoletas

90 días: Madurez

Logs y alertas funcionando, simulacros, métricas de seguridad, playbooks básicos

1 — 2 — 3

60 días: Disciplina

Parches regulares, gestión de vulnerabilidades, endpoints protegidos, terceros controlados

¿Querés que lo armemos en tu empresa?

Diagnóstico inicial + set de controles adaptado + tablero de seguimiento para tu equipo.

Contacto: Formulario web o LinkedIn — Mimetic Advisory