

20 controles ISO 27001 que sí se operan

Guía práctica para equipos de TI y seguridad que quieren cumplimiento real, no papel.
Publicada por JG Sistemas · Javier Gutiérrez · Auditor Interno ISO 27001.

Identidad y accesos (A.5, A.8)

- ☐ MFA obligatorio en cuentas administrativas, VPN y accesos remotos — sin excepciones.
- ☐ Cuentas de servicio con contraseñas rotadas y sin permisos interactivos.
- ☐ 802.1X en LAN y Wi-Fi corporativa con certificados o RADIUS + LDAP.
- ☐ Revisión trimestral de accesos privilegiados con evidencia firmada.
- ☐ Baja de usuarios en <24 h desde RRHH con checklist automatizado.

Perímetro y red (A.8.20 - A.8.23)

- ☐ Segmentación por VLAN entre usuarios, servidores, IoT y OT — con reglas explícitas.
- ☐ Firewalls con reglas revisadas y comentadas; sin regla 'any-any-allow'.
- ☐ Filtrado DNS y bloqueo de C2 conocido en la capa perimetral.
- ☐ IPS activo en Internet-facing y reportes semanales de detecciones.

Endpoint y monitoreo (A.8.7, A.8.16)

- ☐ EDR desplegado en 100% de endpoints y servidores; alertas correlacionadas.
- ☐ SIEM o equivalente con logs de firewall, AD, EDR y VPN — retención mínima 90 días.
- ☐ Playbook de contención documentado y probado al menos una vez al año.

Vulnerabilidades y hardening (A.8.8, A.8.9)

- ☐ Escaneo autenticado mensual; SLA de parcheo por criticidad definido y medido.
- ☐ Baseline de hardening por SO (CIS o equivalente) aplicado a nuevas instalaciones.
- ☐ Inventario de activos actualizado — sin él, ningún control funciona.

Respaldos y continuidad (A.8.13, A.5.30)

- ☐ Respaldo 3-2-1 con al menos una copia offline o inmutable.
- ☐ Prueba de restauración documentada cada trimestre.
- ☐ Plan de continuidad con RTO/RPO por sistema crítico.

Gobierno y evidencia (A.5.1, A.5.36)

- ☐ Políticas revisadas anualmente y firmadas por dirección.
- ☐ Registro de incidentes con lecciones aprendidas — no solo tickets cerrados.

Uso recomendado

Imprime esta hoja o compártela con tu equipo. Marca lo que sí operas hoy — no lo que 'ya tienes escrito'. Un control que no se ejecuta es un hallazgo esperando ser levantado.

¿Necesitas apoyo para cerrar los pendientes? Escríbeme y te acompaño en la operación, no solo en el papel.