RESUMEN DE NORMA · CERT.GT

CIS Controls

Versión 1.0 · Revisado el 11 oct 2026 · TLP:CLEAR · Para: Responsables de TI y de seguridad, en especial de organizaciones pequeñas y medianas.

Los CIS Controls son una lista priorizada de acciones concretas contra los ataques más comunes. Donde otros marcos dicen qué lograr, estos dicen qué hacer primero. Son gratuitos y la versión vigente es la 8.1: 18 controles y 153 salvaguardas.

Los grupos de implementación

Las salvaguardas se reparten en tres grupos acumulativos. Empieza por el primero.

IG1 · Higiene esencial	56 salvaguardas. El mínimo para cualquier organización, pensado para equipos pequeños con poco personal de TI.
IG2	IG1 más 74 salvaguardas. Para organizaciones con personal dedicado a TI y datos sensibles.
IG3	Las 153 salvaguardas. Para organizaciones con especialistas en seguridad y riesgo de ataques dirigidos.

Los 18 controles

1	Inventario y control de los activos de la empresa.
2	Inventario y control del software.
3	Protección de datos.
4	Configuración segura de activos y software.
5	Gestión de cuentas.
6	Gestión del control de acceso.
7	Gestión continua de vulnerabilidades.
8	Gestión de registros de auditoría.
9	Protecciones de correo electrónico y navegador web.
10	Defensas contra malware.
11	Recuperación de datos.
12	Gestión de la infraestructura de red.
13	Monitoreo y defensa de la red.
14	Concientización y capacitación en seguridad.
15	Gestión de proveedores de servicios.
16	Seguridad del software de aplicación.
17	Gestión de respuesta a incidentes.
18	Pruebas de penetración.

Por dónde empezar

- Controles 1 y 2: no puedes proteger lo que no sabes que tienes. Haz el inventario de equipos y programas.
- Control 4: cambia contraseñas de fábrica, activa el bloqueo de pantalla y el firewall de cada equipo.
- Controles 5 y 6: una cuenta por persona, verificación en dos pasos y privilegios de administrador sólo para quien los necesita.
- Control 7: activa las actualizaciones automáticas y revisa cada mes lo que quedó sin parchar.
- Control 11: respaldos automáticos, con una copia fuera de línea y pruebas de restauración.
- Control 14: capacita al personal para reconocer el phishing y reportarlo.

Herramientas gratuitas del CIS

- CIS Benchmarks: guías de configuración segura para sistemas operativos, nube y aplicaciones.
- CIS CSAT: herramienta de autoevaluación para medir el avance por control.
- Tablas de correspondencia con NIST CSF, ISO 27001 y PCI DSS.

Errores frecuentes

- Saltar a controles avanzados sin haber terminado el inventario.
- Medir el avance por herramientas compradas y no por salvaguardas funcionando.
- Hacer el inventario una vez y no mantenerlo.

Texto oficial

CIS Critical Security Controls v8.1, gratuitos en cisecurity.org/controls.

cert.gt es una iniciativa privada y comunitaria de Devel Group.

cert.gt · devel.group · Reporta un incidente en cert.gt/reportar o a incidentes@cert.gt

Resumen elaborado por cert.gt con fines educativos; no es el texto oficial de la norma ni sustituye asesoría legal o de cumplimiento. No es un documento de una entidad gubernamental. Puedes copiarlo y adaptarlo citando la fuente (CC BY 4.0).