ENTIENDE. COMPRUEBA. MEJORA.

¿Qué es un análisis de ciberseguridad?

Un análisis de ciberseguridad es una revisión de cómo protege tu empresa su información y sus sistemas: qué controles tiene, qué evidencias los respaldan y qué conviene mejorar primero. Termina en hallazgos y en un plan de mejora con prioridades, no en un sello ni en una garantía.



Una guía para pasar a la acción

Explicaciones claras, un ejemplo ficticio y una hoja para organizar tus próximas tres acciones.

Consulta la versión web y sus actualizaciones ↗

01 / COMPRENDER

Qué se revisa

- Organización y responsabilidades: quién decide y quién responde.
- Inventario: qué equipos, sistemas y servicios usa la empresa.
- Accesos: cuentas, permisos y autenticación multifactor.
- Equipos: actualizaciones, configuración y protección.
- Red, nube y acceso remoto.
- Datos y copias de seguridad.
- Personas y proveedores.
- Detección y respuesta a incidentes.

02 / COMPRENDER

Análisis, auditoría, pentest y certificación

Estas palabras se usan a menudo como si fueran lo mismo, así que conviene preguntar qué incluye cada propuesta.

- Análisis: revisa controles y evidencias para decidir qué mejorar primero. Puede combinarse con comprobaciones técnicas.
- Auditoría: compara la empresa con una norma o un criterio concreto, siguiendo un método formal.
- Prueba de penetración (pentest): intenta aprovechar fallos de sistemas concretos, con autorización y un alcance acordado. Es una de las técnicas de prueba que describe la guía SP 800-115 del NIST.
- Certificación: la emite una entidad de certificación frente a una norma, como ISO/IEC 27001. Un análisis no la sustituye, aunque puede ayudar a prepararla.

03 / COMPRENDER

Qué debería recibir tu empresa

- Hallazgos con su severidad, indicando hasta dónde se han verificado.
- Un informe ejecutivo que puedas descargar y conservar.
- Un plan de mejora con prioridades y plazos.
- Las limitaciones de la revisión, por escrito.

04 / COMPRENDER

Qué no puede prometer

Ningún análisis puede garantizar que no vayas a sufrir un incidente. Refleja lo revisado, en un momento y con un alcance concretos. Desconfía de los porcentajes de «seguridad» que no explican de dónde salen.

DEL CONOCIMIENTO A LA PRÁCTICA

Llévalo a tu empresa

EJEMPLO FICTICIO

«Tenemos copias» no responde a toda la pregunta

Una empresa ficticia guarda una copia de sus documentos cada noche. Durante la revisión, nadie encuentra una prueba de restauración reciente. El hallazgo no es «no hay copias», sino «no se ha demostrado que se puedan recuperar los documentos».

Una respuesta describe una práctica. Una evidencia permite comprobarla. El plan debe convertir la diferencia en una acción concreta, con responsable y fecha.

01

Antes de empezar

Delimita el alcance

Anota los servicios, equipos, sedes y proveedores que quieres revisar. Pregunta qué queda fuera y qué accesos serían necesarios.

02

Durante la revisión

Prepara evidencias útiles

Reúne inventarios, políticas y registros de pruebas. Comparte solo lo necesario por el canal acordado; no envíes contraseñas ni claves secretas.

03

Al recibir el informe

Asigna las primeras acciones

Elige las prioridades según impacto y esfuerzo. Define quién hará cada tarea, para cuándo y cómo se comprobará que funciona.

Qué conviene conservar

Una lista de hallazgos con alcance, evidencia, responsable, fecha objetivo y criterio de cierre. Una tarea cerrada debe explicar qué se verificó.

TU HOJA DE TRABAJO

Tres acciones. Un siguiente paso.

Completa esta hoja con tu equipo. Define cómo comprobaréis cada mejora. No anotes contraseñas, claves ni información confidencial.

01 / Acción

Responsable: _____ Fecha: _____

Cómo comprobarla: _____

02 / Acción

Responsable: _____ Fecha: _____

Cómo comprobarla: _____

03 / Acción

Responsable: _____ Fecha: _____

Cómo comprobarla: _____

Preguntas frecuentes

¿Un análisis sustituye a una auditoría de cumplimiento?

No. Ayuda a entender el estado real y a prepararse, pero no certifica el cumplimiento de ninguna norma.

¿Hace falta dar acceso a los sistemas?

Depende del alcance. Evaleris Esencial analiza tus controles y tus evidencias, sin escanear tus sistemas. Las comprobaciones técnicas de Evaleris Integral requieren tu autorización y un alcance acordado.

Fuentes y siguiente paso

- NIST SP 800-115: Technical Guide to Information Security Testing and Assessment ↗

Mira paso a paso cómo lo hacemos, desde el alcance hasta el plan de mejora. Ver cómo funciona ↗

Información general. No es una auditoría, una certificación ni una garantía de seguridad. Ejemplos ficticios. Edición: 5 de noviembre de 2026.