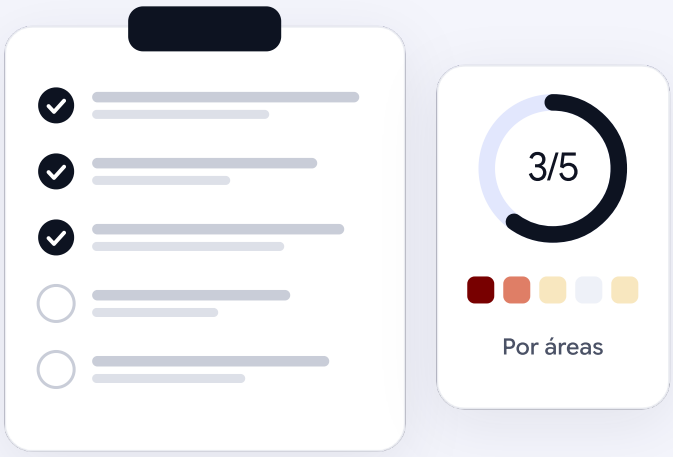
ENTIENDE. COMPRUEBA. MEJORA.

Lista de comprobación de ciberseguridad para empresas

Estas 15 preguntas cubren lo básico: accesos, equipos, copias de seguridad, información y personas. Si no puedes responder «sí» a alguna, ya sabes por dónde empezar. No sustituye a un análisis profesional, pero es una primera orientación honesta.



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

Accesos y permisos

Quién puede entrar en tus sistemas, con qué permisos y cómo se comprueba que es quien dice ser.

- [ ] ¿Es obligatoria la autenticación multifactor para todas las cuentas de administrador?
- [ ] ¿Cada persona dispone únicamente de los permisos necesarios para su trabajo?
- [ ] ¿Se retiran de forma oportuna los accesos cuando alguien deja la empresa o cambia de función?
- [ ] ¿El acceso remoto a los sistemas de la empresa está protegido y limitado a quien lo necesita?

02 / COMPRENDER

Equipos y sistemas

Qué equipos y servicios usa tu empresa, si están al día y si están protegidos.

- [ ] ¿Hay una lista actualizada de los equipos, los sistemas y los servicios en la nube que usa la empresa?
- [ ] ¿Existe un proceso para aplicar las actualizaciones de seguridad de los equipos y sistemas?
- [ ] ¿Los equipos de trabajo cuentan con protección de seguridad activa y mantenida?

03 / COMPRENDER

Copias de seguridad

Si podrías recuperar tu información esencial después de un ataque o de un error.

- [ ] ¿Se realizan copias de seguridad periódicas de la información esencial para el negocio?
- [ ] ¿Se ha comprobado que se puede restaurar información importante desde las copias de seguridad?

04 / COMPRENDER

Información, pagos y proveedores

Cómo se comparte la información sensible, se verifican los pagos y se controla a los proveedores.

- [ ] ¿El equipo utiliza canales aprobados para compartir información sensible?
- [ ] ¿Se verifican por un canal independiente los cambios de cuenta bancaria o las solicitudes de pago inusuales?
- [ ] ¿Se sabe qué proveedores acceden a los datos o sistemas de la empresa, y se revisa su seguridad?

05 / COMPRENDER

Personas y respuesta

Si tu equipo sabe reconocer un engaño, a quién avisar y quién coordina la respuesta.

- [ ] ¿Las personas saben dónde y cómo reportar un correo sospechoso o un posible incidente?
- [ ] ¿El equipo recibe formación práctica de ciberseguridad adecuada a sus funciones?
- [ ] ¿Está definido quién coordina la respuesta cuando ocurre un incidente de seguridad?

DEL CONOCIMIENTO A LA PRÁCTICA

Llévalo a tu empresa

EJEMPLO FICTICIO

«No lo sé» también sirve para avanzar

En este ejercicio ficticio, la dirección desconoce si se han probado las copias. No hace falta adivinar ni responder «sí» porque alguien cree que están configuradas. Se registra la duda, se asigna un responsable y se pide el resultado de la última restauración.

Esta lista ayuda a abrir conversaciones y localizar tareas. No convierte el número de respuestas afirmativas en un porcentaje de seguridad ni demuestra cumplimiento.

01

Primera revisión

Responde con lo que sabes

Recorre las cinco áreas con quienes gestionan los sistemas y las operaciones. Distingue lo comprobado de lo que todavía depende de una suposición.

02

Siguiente paso

Elige tres prioridades

Valora qué podría interrumpir el trabajo, exponer información o facilitar un fraude. Elige acciones concretas, con un responsable y una fecha realista.

03

Revisión acordada

Comprueba el avance

Vuelve a las respuestas pendientes y pide evidencias. Si cambian los sistemas, los proveedores o el equipo, revisa también las prácticas afectadas.

Qué conviene conservar

Para cada prioridad: qué debe cambiar, quién lo hará, fecha objetivo y cómo se verificará. El PDF incluye una hoja para escribir estas tres acciones.

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

¿Esta lista sirve para cumplir una norma?

No. Es una primera orientación sobre buenas prácticas, y no demuestra el cumplimiento de ninguna norma.

¿Puedo obtener un resultado con estas preguntas?

Sí. Son las del análisis inicial gratuito: al responderlas recibes tus prácticas declaradas por área y tres primeras acciones.

Fuentes y siguiente paso

- INCIBE: Los hábitos de la pyme ciberresiliente ↗

Responde estas mismas preguntas y recibe tu orientación por áreas. Hacer el análisis gratuito ↗

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