PROTEO
smart protect

CHECKLIST EJECUTIVO

¿Necesitas un Plan Director de Seguridad?

20 preguntas para saber si tu organización tiene una dirección clara en ciberseguridad o está actuando de forma reactiva.

Para pymes, administraciones públicas y entidades del tercer sector

Diagnóstico orientativo. No sustituye una auditoría.

INTELIGENCIA Y PROTECCIÓN

ANTES DE EMPEZAR

Una conversación de dirección, no un examen técnico

El objetivo es detectar si la organización puede responder con claridad a las decisiones básicas de seguridad. Reúne a dirección y a las personas responsables de tecnología, administración o protección de datos.

Puntuación

NO / NO LO SABEMOS	PARCIAL	SÍ, Y HAY EVIDENCIA
0 puntos	**1 punto**	**2 puntos**

Una respuesta vale más cuando puede demostrarse

Una política sin responsables, una copia sin pruebas de restauración o un inventario sin actualizar deben marcarse como parciales. El Plan Director se apoya en evidencias y capacidad real, no solo en intenciones.

Resultado

Suma los puntos al finalizar. La puntuación no mide cumplimiento ni madurez de forma certificable: ayuda a decidir si necesitas un diagnóstico más profundo y una hoja de ruta.

RESPONDE CON EVIDENCIA

BLOQUE 1

Gobierno y contexto

01	¿La dirección ha definido qué objetivos de negocio debe proteger la ciberseguridad?	☐ No	☐ Parcial	☐ Sí
02	¿Existe una persona responsable de coordinar la seguridad y con autoridad para impulsar acciones?	☐ No	☐ Parcial	☐ Sí
03	¿Conocéis qué servicios, procesos y datos son esenciales para seguir funcionando?	☐ No	☐ Parcial	☐ Sí
04	¿Tenéis identificadas las obligaciones aplicables, incluidas las contractuales y sectoriales?	☐ No	☐ Parcial	☐ Sí

BLOQUE 2

Activos, accesos y terceros

05	¿Existe un inventario actualizado de equipos, aplicaciones, cuentas, datos y servicios cloud?	☐ No	☐ Parcial	☐ Sí
06	¿Los accesos se conceden, revisan y retiran mediante un procedimiento definido?	☐ No	☐ Parcial	☐ Sí
07	¿Se conocen los proveedores que pueden acceder a datos o sistemas críticos?	☐ No	☐ Parcial	☐ Sí
08	¿Los activos y dependencias están clasificados según su importancia para la organización?	☐ No	☐ Parcial	☐ Sí

RESPONDE CON EVIDENCIA

BLOQUE 3

Continuidad y recuperación

09	¿Las copias de seguridad cubren los datos y sistemas realmente críticos?	☐ No	☐ Parcial	☐ Sí
10	¿Se realizan pruebas periódicas de restauración y se conservan evidencias del resultado?	☐ No	☐ Parcial	☐ Sí
11	¿La organización sabe cuánto tiempo puede permanecer sin sus servicios esenciales?	☐ No	☐ Parcial	☐ Sí
12	¿Existen responsables y procedimientos para actuar ante una interrupción grave?	☐ No	☐ Parcial	☐ Sí

BLOQUE 4

Vulnerabilidades e incidentes

13	¿Las vulnerabilidades se detectan, priorizan y corrigen según el riesgo?	☐ No	☐ Parcial	☐ Sí
14	¿Existe un procedimiento conocido para notificar, clasificar y gestionar incidentes?	☐ No	☐ Parcial	☐ Sí
15	¿Se registran los incidentes y se utilizan las lecciones aprendidas para mejorar?	☐ No	☐ Parcial	☐ Sí
16	¿La exposición externa, los accesos remotos y las configuraciones críticas se revisan periódicamente?	☐ No	☐ Parcial	☐ Sí

RESPONDE CON EVIDENCIA

BLOQUE 5

Personas, evidencias y mejora

17	**¿La formación se adapta a los riesgos y responsabilidades de cada perfil?**	☐ No	☐ Parcial	☐ Sí
18	**¿Las políticas y procedimientos se revisan, aprueban y comunican de forma efectiva?**	☐ No	☐ Parcial	☐ Sí
19	**¿Cada medida de seguridad tiene responsable, plazo e indicador de seguimiento?**	☐ No	☐ Parcial	☐ Sí
20	**¿La dirección recibe información periódica para decidir prioridades e inversión?**	☐ No	☐ Parcial	☐ Sí

Mi resultado

Puntuación total ☐ / 40 puntos

Preguntas sin respuesta clara ☐

Decisiones que debemos aclarar

SUMA Y CONVERSA

¿Qué te dice la puntuación?

32-40
PUNTOS

Base controlada

Existe una base de gobierno. El Plan Director puede ayudarte a consolidar, medir y ordenar los siguientes proyectos.

20-31
PUNTOS

Brechas relevantes

Hay controles, pero también decisiones sin cerrar. Es recomendable priorizar riesgos, responsables y una hoja de ruta común.

0-19
PUNTOS

Gestión reactiva

La organización depende demasiado de respuestas puntuales. Conviene realizar un diagnóstico y definir prioridades antes de seguir invirtiendo.

No te quedes solo con el número

Anota las respuestas que han generado desacuerdo, dudas o un 'no lo sabemos'. Esas conversaciones suelen revelar las primeras decisiones que debe ordenar un Plan Director.

DEL DIAGNÓSTICO A LA EJECUCIÓN

Lo que debe producir un buen Plan Director

01 Diagnóstico ejecutivo

Situación actual, activos críticos, dependencias y principales brechas.

02 Mapa de riesgos priorizado

Escenarios ordenados por impacto, probabilidad, urgencia y tolerancia.

03 Hoja de ruta por fases

Medidas inmediatas, horizonte de 90 días y consolidación anual.

04 Cartera de proyectos

Alcance, responsables, esfuerzo, indicadores y evidencias esperadas.

PRINCIPIO PROTEO

Primero justificamos la necesidad.
Después elegimos la solución.

La ciberseguridad debe responder al riesgo y a la capacidad real de la organización.

Poner orden es el primer proyecto de seguridad.

Si este checklist ha dejado preguntas abiertas, podemos ayudarte a convertirlas en un diagnóstico, una hoja de ruta y una cartera de proyectos ejecutable.

Solicita una primera valoración

proteo-tech.com/contact/

Nota de alcance

Este checklist es una herramienta orientativa de concienciación y toma de decisiones. No constituye una auditoría, un análisis de riesgos formal, asesoramiento jurídico ni una garantía de cumplimiento de ENS, NIS2, RGPD o ISO 27001.

Referencia metodológica: INCIBE - Plan Director de Seguridad para empresas
incibe.es/empresas/que-te-interesa/plan-director-seguridad