GUÍA DE TRABAJO

NIS2 y tu empresa

Preparar la revisión técnica y de alcance

Preguntas, inventario y evidencias para
preparar una revisión con responsables.
No determina obligaciones ni certifica cumplimiento.

1
inventario
de activos

2
ámbitos: técnico
y normativo

3
prioridades
por acordar

BenusTech
Software, cloud e IA aplicada a empresas

benustech.es · info@benustech.es · +34 694 275 853

Esta guía ayuda a preparar información para revisar ciberseguridad y el posible encaje de NIS2. No permite decidir por sí sola si una empresa está dentro o fuera del ámbito, ni sustituye el análisis especializado de la normativa vigente.

Qué conviene separar

La Directiva (UE) 2022/2555 es una referencia normativa europea. La aplicabilidad a una entidad requiere revisar actividad, tamaño, excepciones, relaciones y normativa nacional o sectorial pertinente. No afirmamos un estado actual de transposición, un umbral universal ni una sanción aplicable a tu empresa.

> **Fuente primaria**
> Texto oficial: https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963. Contrasta la versión y la legislación aplicable en la fecha de la revisión. Esta guía no es un dictamen jurídico.

Información para evaluar el alcance

- Entidad y actividades efectivamente realizadas
- Servicios prestados y dependencias de proveedores
- Características de la empresa y relaciones con otras entidades
- Contratos y requisitos de clientes o administraciones
- Responsable que revisará el encaje normativo

Un requisito contractual de un cliente y una obligación legal directa son cuestiones distintas. No presupongas que tener pocos empleados excluye cualquier obligación, ni que trabajar con una entidad regulada convierte automáticamente a todos sus proveedores en entidades reguladas.

Inventario técnico que puedes preparar

Elemento	Qué reunir
Aplicaciones y datos	Uso, responsable, criticidad y accesos
Identidades	Altas, bajas, privilegios y cuentas de servicio
Copias	Alcance, conservación y pruebas de restauración
Proveedores	Dependencias y contactos de operación
Incidentes	Procedimiento, responsabilidades y evidencias

Controles y pruebas

Distingue lo recomendado de lo implantado y de lo probado. Registrar que existe una copia no demuestra que se haya restaurado. Una herramienta de seguridad o una certificación del proveedor no acreditan por sí solas el cumplimiento de la empresa.

1. Identificar riesgos y procesos afectados
2. Proponer controles y responsables
3. Acordar prioridades, coste y aceptación
4. Ejecutar pruebas en un entorno autorizado
5. Registrar resultados, límites y trabajo pendiente

Respuesta y comunicación

Define quién detecta, decide, conserva evidencias y coordina la recuperación. Las obligaciones y plazos de notificación deben revisarse para el incidente y la entidad concretos; no se deducen de esta guía. No se incluye una promesa de atención permanente o respuesta en un plazo fijo.

> **Resultado de la revisión**
> El entregable útil es un inventario, riesgos priorizados, controles con responsables y pruebas identificadas. El análisis jurídico y la aprobación de cumplimiento requieren su propio responsable competente.