Checklist de cumplimiento NIS2

Saber qué pide NIS2 es una cosa; saber si ya lo cumples es otra. Esta checklist recorre, bloque a bloque, lo que el departamento de IT debería poder enseñar en una auditoría.

Marca cada punto cuando lo tengas resuelto.

Antes de empezar: ¿estás dentro?

- [ ] Confirma con tu asesoría legal si tu organización es entidad esencial, importante o ninguna de las dos.
- [ ] Revisa qué exigen tus clientes: muchos piden estas medidas a sus proveedores aunque la ley no te obligue.
- [ ] Nombra a una persona responsable de coordinar el cumplimiento.

1. Gobierno y responsabilidades

- [ ] La dirección ha aprobado la política de seguridad y las medidas de gestión de riesgos.
- [ ] Hay un responsable de seguridad con funciones definidas por escrito.
- [ ] La dirección ha recibido formación en ciberseguridad y queda constancia.
- [ ] Existe un calendario de revisión de las medidas, al menos anual.

2. Inventario y análisis de riesgos

- [ ] Inventario actualizado de equipos, servidores, servicios cloud y aplicaciones.
- [ ] Inventario de licencias y de a quién están asignadas.
- [ ] Lista de cuentas de usuario y de quién tiene acceso a qué, incluidas las cuentas con privilegios.
- [ ] Análisis de riesgos documentado, con los activos críticos identificados.
- [ ] Plan de tratamiento: qué riesgo se acepta, cuál se reduce y con qué medida.

3. Medidas técnicas

- [ ] Autenticación multifactor en el correo, el acceso remoto y las cuentas con privilegios.
- [ ] Parches de sistemas y aplicaciones al día, con un plazo definido para los críticos.
- [ ] Protección de los dispositivos y detección de amenazas.
- [ ] Cifrado de portátiles y de los datos sensibles.
- [ ] Copias de seguridad automáticas, con al menos una copia fuera de la red principal, y pruebas de restauración periódicas.
- [ ] Plan de continuidad y de recuperación ante desastres.
- [ ] Comunicaciones seguras para las emergencias.

4. Gestión y notificación de incidentes

24 h
Alerta temprana
Primer aviso de que algo ha ocurrido.

72 h
Notificación
Evaluación inicial de la gravedad y el impacto.

1 mes
Informe final
Un mes después de la notificación: descripción, causa raíz, medidas de mitigación e impacto transfronterizo.

- [ ] Procedimiento escrito para detectar, clasificar y gestionar incidentes.
- [ ] Criterios claros para decidir si un incidente es significativo.
- [ ] Responsables y suplentes para notificar, con sus contactos a mano.
- [ ] Plantillas preparadas para los tres avisos que pide la directiva
- [ ] Registro de cada incidente, con su cronología y las medidas tomadas.
- [ ] Un simulacro al año para comprobar que el procedimiento funciona.

5. Proveedores y cadena de suministro

- [ ] Lista de proveedores con acceso a sistemas o datos, y de los servicios críticos que prestan.
- [ ] Cláusulas de seguridad y de notificación de incidentes en sus contratos.
- [ ] Revisión periódica de su nivel de seguridad, proporcional al riesgo.
- [ ] Fechas de renovación controladas, para revisar las condiciones antes de que se renueven solas.

6. Formación y concienciación

- [ ] Formación básica en ciberseguridad para toda la plantilla, al menos una vez al año.
- [ ] Formación específica para quien administra sistemas o gestiona incidentes.
- [ ] Simulacros de phishing y seguimiento de los resultados.
- [ ] Buenas prácticas de ciberhigiene por escrito: contraseñas, dispositivos, correo y teletrabajo.
- [ ] Altas y bajas con los accesos revisados: nadie conserva permisos después de irse.

7. Evidencias: cómo demostrarlo

- [ ] Las políticas aprobadas, con fecha y firma.
- [ ] El inventario y el análisis de riesgos, con su última revisión.
- [ ] Los registros de incidentes y de simulacros.
- [ ] Los resultados de las pruebas de restauración.
- [ ] Los registros de formación de la plantilla y de la dirección.
- [ ] Los contratos de proveedores con sus cláusulas de seguridad.

Esta checklist es orientativa y no sustituye al asesoramiento legal. Versión explicada:
monkinet.ai/blog/checklist-cumplimiento-nis2