CHECKLIST

Checklist: Evaluación de controles NIS2

Evaluación de cumplimiento de la Directiva NIS2 en entornos Microsoft 365 y Azure.

Kwadrant Systems — Marzo 2026

La Directiva NIS2 (transpuesta en España mediante la Orden PJC/522/2025) amplía las obligaciones de ciberseguridad a más sectores y empresas. Este checklist permite evaluar el estado de cumplimiento de los controles técnicos exigidos, utilizando herramientas del ecosistema Microsoft.

Sectores afectados por NIS2

NIS2 distingue entre entidades esenciales y entidades importantes:

Categoría	Sectores
Esenciales	Energía, transporte, banca, salud, agua, infraestructura digital, administración pública, espacio
Importantes	Servicios postales, residuos, industria química, alimentación, fabricación, proveedores digitales, investigación

1. Gestión de riesgos

- ■ Existe un análisis de riesgos documentado y actualizado
- ■ Se han identificado los activos críticos y sus dependencias
- ■ Hay un responsable de seguridad designado
- ■ Se revisan los riesgos al menos anualmente

2. Gestión de incidentes

- ■ Existe un plan de respuesta a incidentes documentado
- ■ El equipo conoce el procedimiento de notificación (24h alerta, 72h informe)
- ■ Se realizan simulacros al menos una vez al año

- ■ Hay un sistema de registro y seguimiento de incidentes
- ■ Alertas automáticas configuradas en Defender / Sentinel

3. Continuidad de negocio

- ■ Existe un plan de continuidad documentado
- ■ Hay backup independiente con pruebas de recuperación periódicas
- ■ RPO y RTO están definidos por servicio
- ■ Se realizan pruebas de restauración con acta firmada

4. Cadena de suministro

- ■ Se han identificado los proveedores críticos y sus riesgos
- ■ Existen contratos con cláusulas de seguridad
- ■ El acceso de terceros es controlado y auditable
- ■ Se revisan los accesos de proveedores periódicamente

5. Adquisición y desarrollo

- ■ Los nuevos sistemas se evalúan antes del despliegue
- ■ Existe un proceso de gestión de vulnerabilidades
- ■ Las actualizaciones se aplican en plazos definidos

6. Formación y concienciación

- ■ Existe un programa de concienciación en ciberseguridad
- ■ Se realizan simulaciones de phishing periódicas
- ■ El personal técnico recibe formación específica
- ■ Hay un registro de formaciones realizadas

7. Cifrado y control de acceso

- ■ MFA activo para todos los usuarios
- ■ Acceso condicional configurado
- ■ Cifrado en tránsito y en reposo implementado

- Gestión de privilegios con elevación temporal (PIM)
- Revisiones de acceso programadas

8. Notificación de incidentes

- Procedimiento de notificación a CSIRT documentado
- Plazos conocidos: 24h alerta, 72h informe, 1 mes final
- Plantillas de notificación preparadas
- CSIRT de referencia identificado

Contacto: kwadrant.es — Evaluación NIS2 gratuita