



WEBINAR

Miércoles, 18 de marzo de 2026 - 10:00h.

DIRECTIVA NIS2:

Claves para el cumplimiento normativo
y la ciberseguridad empresarial



ORGANIZA:



Cofinanciado por
la Unión Europea



MINISTERIO
DE HACIENDA



Fondos Europeos



Gobierno
de Canarias

Consejería de Universidades,
Ciencia e Innovación y Cultura

Agencia Canaria de Investigación,
Innovación y Sociedad
de la Información



COLABORA:



DIRECTIVA NIS2

Las claves para el
cumplimiento normativo y la
ciberseguridad empresarial



¿Qué es la Directiva NIS2?

La NIS2 es una directiva de la Unión Europea cuyo fin principal es mejorar la ciberseguridad en sectores clave y críticos.

- ✓ Sustituye a NIS 1
- ✓ Aprobada en 2022



Objetivos de la directiva

- ✓ Mejorar la ciberseguridad en la UE
- ✓ Ampliar el alcance a sectores críticos
- ✓ Aumentar la responsabilidad de las empresas
- ✓ Establecer medidas mínimas de seguridad
- ✓ Garantizar notificación rápida de incidentes
- ✓ Fomentar la cooperación europea
- ✓ Reducir riesgos y proteger la economía y sociedad

NIS2 – Fechas clave

16 enero 2023

Entrada en
vigor de la
directiva en la
Unión Europea

17 de octubre 2024

Límite para la
trasposición al
ordenamiento
jurídico de los
Estados Miembros

14 de enero de 2025

El Gobierno español
aprueba el borrador
del anteproyecto de
ley que incorpora
NIS2

¿La directiva es de obligatorio cumplimiento en España?

Actualmente, aún no se ha aprobado el anteproyecto de ley en España que incluye NIS2, pero se espera que lo esté durante este mismo año 2026.

Por tanto, las empresas ya deben prepararse para su cumplimiento para evitar sanciones y reforzar su protección digital.



Ámbitos de aplicación

NIS2 distingue entre **entidades esenciales** e **importantes** según sector y tamaño de la organización, y establece qué sectores están cubiertos dentro de su ámbito de aplicación.



Entidades esenciales: organizaciones de sectores críticos obligadas a cumplir NIS2 siempre que sean grandes o estratégicas.



Entidades importantes: organizaciones de sectores relevantes que solo deben cumplir NIS2 si cumplen determinados criterios de tamaño o impacto.

Quedan excluidas de la aplicación de NIS2 las microempresas y pequeñas empresas que no pertenezcan a sectores esenciales o importantes.

Entidades esenciales



Energía (electricidad, petróleo, gas)



Salud y servicios sanitarios (hospitales, laboratorios, servicios de emergencia)



Finanzas (banca, infraestructuras de mercado financiero)



Administración pública



Infraestructura digital (telecomunicaciones, DNS, TLD, cloud, centros de datos)



Agua potable y tratamiento de aguas residuales



Transporte (aéreo, ferroviario, marítimo, carretera)



Espacio y servicios satelitales

Entidades importantes



Proveedores de servicios digitales
(marketplaces, motores de búsqueda,
RR.SS.)



Servicios postales y de mensajería



Gestión de residuos



Producción, procesamiento y
distribución de alimentos



Manufactura de productos críticos (dispositivos
médicos, electrónica, maquinaria, vehículos)



Industria química



Investigación y organizaciones de
investigación

Obligaciones para empresas

- ✓ Medidas de seguridad proporcionales al riesgo del sector
- ✓ Gestión de riesgos de ciberseguridad
- ✓ Notificación de incidentes significativos
- ✓ Responsabilidad de la alta dirección
- ✓ Cooperación con autoridades competentes y CSIRT
- ✓ Aplicación a entidades esenciales e importantes

Supervisión bajo NIS2

Cada Estado miembro debe designar autoridades competentes (entidades públicas o agencias reguladoras) para supervisar el cumplimiento de NIS2 a través de:

- ✓ Inspecciones in situ o a distancia para verificar cumplimiento
- ✓ Auditorías de seguridad periódicas o específicas
- ✓ Análisis de seguridad para identificar vulnerabilidades y riesgos
- ✓ Solicitudes de información sobre medidas de ciberseguridad
- ✓ Pruebas de cumplimiento con evidencias de políticas de seguridad

Las autoridades competentes evaluarán el cumplimiento de las medidas de seguridad y la gestión de riesgos.



Riesgos de incumplimiento



Sanciones económicas y legales



Responsabilidad legal de la alta dirección



Interrupciones en los servicios



Pérdida de confianza y daño reputacional



Exposición a ciberataques y brechas de seguridad



Incumplimiento de acuerdos contractuales



Impacto en la cadena de suministro



Falta de capacidad para gestionar incidentes

Desafíos técnicos para el cumplimiento normativo

LOS OBSTÁCULOS DE LA DIGITALIZACIÓN



Principales retos que enfrentamos



40%

Visibilidad limitada del entorno de TI



39%

Falta de conocimiento para responder a incidentes



48%

Dificultades para adaptar los programas de formación de empleados



35-44%

Falta de personal cualificado



32%

Riesgo de seguridad en aplicaciones Legacy



Guía para cumplir con la Directiva NIS2

PASOS DEL CUMPLIMIENTO NORMATIVO

NIS2 Roadmap





Herramientas para asegurar el cumplimiento normativo

CÓMO ADECUARTE A NIS2

Nuestro conocimiento y reconocimiento

Microsoft Cloud Partner Program: Solution Areas



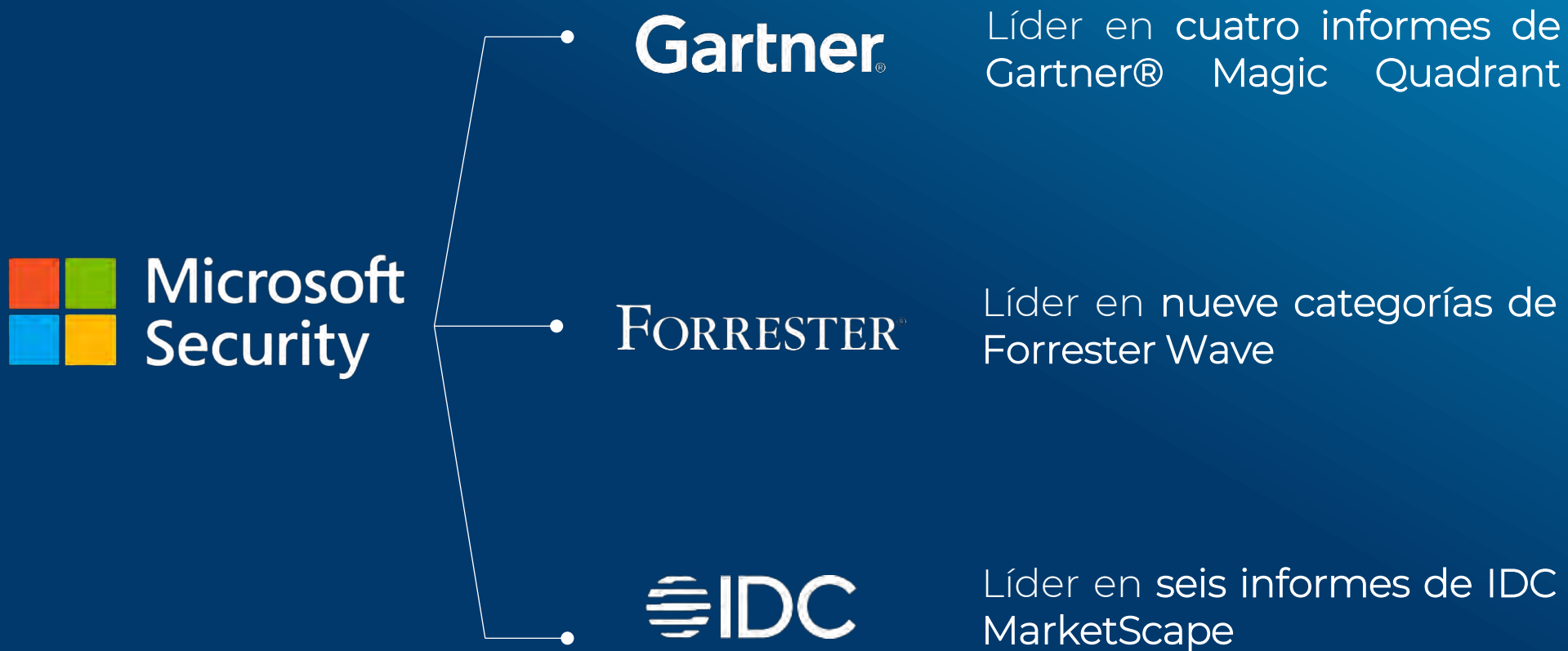
Security and Compliance



Certificaciones profesionales de seguridad



Microsoft Security: el líder del compliance



CONTIGO EN CADA PASO

Las soluciones de Intelequia para cada principio NIS

Principios NIS	Solución de Intelequia
Gobernanza	Servicios Gestionados (Infraestructura, M365)
Gestión de riesgos	Servicios Gestionados M365
Gestión de activos	Servicios Gestionados (Infraestructura, M365)
Supply chain	Servicios Gestionados (Infraestructura, M365) + Auditorías de Seguridad
Protección de un servicio	Servicios Gestionados Infraestructura + Auditorías de Seguridad
Identidad y acceso	Servicios Gestionados M365
Seguridad de los datos	Servicios Gestionados (Infraestructura, M365) + ThunderCloud Backup
Seguridad de sistemas	Servicios Gestionados Infraestructura
Redes resilientes	Servicios Gestionados Infraestructura
Conciencia del personal	Formación + Concienciación
Política de gestión de incidentes de seguridad	Servicio de SOC
Seguridad proactiva	Servicios Gestionados (Infraestructura, M365) + Servicio de SOC + Auditorías de Seguridad
Respuesta y recuperación	Servicio de SOC + ThunderCloud Backup + Servicios Gestionados (Infraestructura, M365)

INFRASTRUCTURA CLOUD

Servicios Gestionados Infraestructura

No sobrecargues tu departamento TI. Nos ocupamos de la gestión, mantenimiento y soporte de tus servicios en Azure



Monitorización activa

Para los servicios activos en Azure con alertas de incidencias



Control de máquinas virtuales

Adaptadas a de cada hardware y software



Soporte técnico

Configuración, actualización y despliegue para los servicios de Azure



Respuesta ante incidentes

Para los servicios de Azure desplegados



Asesoramiento técnico continuo

Arquitecto Cloud especialista en Azure garantiza la optimización de seguridad IT y costes



COPIAS DE SEGURIDAD EN LA NUBE

ThunderCloud Backup

- ✓ Solución robusta y eficiente para tus copias de seguridad en la nube y recuperación de desastres
- ✓ Interfaz de usuario amigable
- ✓ Automatización de backups de infraestructura y M365
- ✓ Cifrado avanzado para proteger tus datos
- ✓ Gestión y monitorización 24/7

EL VALOR DE ESTAR SIEMPRE PROTEGIDO

Servicios Gestionados M365



Protección integral de identidad

Correo, dispositivos y datos



Fortalece y blindas tu tenant

Cierre de brechas y refuerzo continuo de la configuración de seguridad



Optimización y cumplimiento continuo

Según cambios de Microsoft y marcos como CIS o NIST, con informes listos para auditorías



Soporte experto proactivo

Expertos en M365 dedicados a la supervisión, configuración y mejora continua de tu entorno



Visión completa y control centralizado

Paneles, métricas e informes para gestionar con datos y sin sorpresas

Cobertura total de seguridad en M365

Nuestro servicio protege cada capa de tu entorno Microsoft 365, desde la identidad y los dispositivos hasta el correo, aplicaciones y datos. Obtén backups y restauraciones de tus configuraciones.



Seguridad de Dispositivos e Intune

Configuración segura, cumplimiento, actualizaciones, cifrado, protección antivirus y EDR.



Correo y Exchange Online

Anti-spam, anti-phishing, anti-malware, protección de enlaces y adjuntos.



Identidad y Entra ID

Acceso condicional, grupos de seguridad, autenticación multifactor, privilegios mínimos.



Microsoft 365 Apps y SharePoint/OneDrive

Configuración segura, control de compartición, backup de configuración.



Protección de datos

Políticas de DLP, cifrado de disco, reducción de superficie de ataque.



Defensa avanzada

Microsoft Defender XDR, indicadores y detecciones personalizadas.



Servicio SOC

Monitorización 24/7 y respuesta rápida a amenazas en tiempo real para proteger tu infraestructura

Auditorías de seguridad

Pruebas de penetración (Pentesting) para identificar y corregir vulnerabilidades en tus sistemas, y garantizar seguridad y protección continua contra ataques

Gestión y seguridad en Azure

Implementación y gestión de soluciones seguras en Azure (Intune, Sentinel, y Defender). Protección, monitoreo y respuesta ante amenazas con cumplimiento normativo y seguridad de los datos (Purview) y cloud apps

¿Quieres más información?

intelequia.com

+34 918 336 775 | +34 936 421 692

sales@intelequia.com

Madrid | Barcelona | Canarias | Newark



¿TIENES ALGUNA DUDA?

Preguntas





¡Gracias!

intelequia.com

