



SEMINARIO

De la teoría a la práctica: cómo empezar a prepararse para NIS2

Francisco Lázaro

Presentación del docente



Francisco Lázaro Anguís

Gerente de Área de Ciberseguridad y Privacidad (CISO y DPO) del Grupo Renfe.

Ingeniero de Telecomunicación por la UPM

Master en Protección de Datos y Seguridad de la Información por la UCM

Profesor Asociado en la ETSI de telecomunicaciones de la UPM

Cruz de la Orden del Mérito de la Guardia Civil , con distintivo Blanco

Vocal en el Foro Nacional de Ciberseguridad

Vocal en la mesa de representantes sectoriales de operadores esenciales, Secretaria de Estado de interior.

Habilitado por el Mº del interior como Director de Seguridad.

Galardonado con los premios ASLAN, SIC y Huella, entre otros

Presidente del Grupo de Calidad y Seguridad de AUTELSI.

Director del Centro de Estudios de Movilidad e IoT . Co-director del Grupo de IA y Ciberseguridad del ISMS Forum.

Miembro de la Juntas Directivas de la Asociación ISMS Forum y de la Asociación Española de Ejecutivos y Financieros

Miembro de tres grupos de Normalización UNE e ISO.

Profesor en diversos Masters Universitarios de Ciberseguridad y de Protección de Datos (UCM, UC3M, entre otros)

Contenido

1. Enfoque normativo y destinatarios de la guía
2. Contexto NIS2.
3. Obligaciones normativas y estructura de cumplimiento
4. Comparativa entre NIS2 y APL Española
5. Método de implantación en 12 pasos
6. Desarrollo operativo de los artículos 21 NIS2 y 19 APL
7. Paquetes implantables para cumplir NIS2/APL
8. Roadmap de implantación y checklist de adopción
9. Cuadro de mando y errores habituales en la implantación
10. Ejemplo de paquete de asunción de responsabilidad de los órganos de dirección

Enfoque normativo y
destinatarios de la guía



**Nota
inicial:**

La adopción de la NIS2, por una organización dependerá de múltiples factores: el liderazgo de los Órganos de Dirección, si es sancionable o no, si presta los servicios en competencia real, la capacidad de dotarse de Organización, estructura y recursos, el grado de madurez en Ciberseguridad que tenga de partida.....

Orientación de la guía y destinatarios

Guía paso a paso

La guía ofrece un enfoque para implementar NIS2/APL en la práctica, facilitando la adaptación normativa.

Foco en artículos clave

Se centra en el artículo 21 de la Directiva NIS2 y el artículo 19 del Anteproyecto español para cumplimiento específico.

Destinatarios principales

Orientado a CISOs, RSI, Responsables de cumplimiento, Responsables de SOC/CSIRT, continuidad, compras, jurídico y órganos de dirección.

Contexto NIS2



LEGISLACIÓN EN CIBERSEGURIDAD EN EUROPA

COHERENCIA CON LAS DISPOSICIONES POLÍTICAS EXISTENTES EN EL ÁMBITO DE ACTUACIÓN

La Unión ha ampliado sus instrumentos jurídicos y políticos con la adopción de una serie de instrumentos legales y medidas políticas:

i DIRECTIVA NIS 2 Refuerza la ciberseguridad de los servicios esenciales 	ii DIRECTIVA CER Las medidas de seguridad física se definen en su «directiva hermana». 	iii LEY DE RESILIENCIA CIBERNÉTICA (CRA) Mejora la ciberseguridad de los productos. 	iv LEY DE SOLIDARIDAD CIBERNÉTICA (CSoA) Desarrolla capacidades de respuesta a escala de la UE. 
v PLAN DE ACCIÓN CIBERNÉTICA DE LA UE Apoya la cooperación en materia de gestión de crisis a escala de la UE. 	vi CAJA DE HERRAMIENTAS DE CIBERSEGURIDAD 5G Respalda la ciberseguridad en las redes 5G. 	vii PLAN DE ACCIÓN EUROPEO SOBRE CIBERSEGURIDAD EN HOSPITALES Y PROVEEDORES DE ASISTENCIA SANITARIA 	viii ACADEMIA DE COMPETENCIAS EN CIBERSEGURIDAD Aborda el creciente desafío que supone la falta de personal cualificado en ciberseguridad. 



EL MARCO JURÍDICO DE CIBERSEGURIDAD SE COMPLEMENTA CON LEGISLACIÓN ESPECÍFICA PARA CADA SECTOR



REGLAMENTO DORA

Ley de Resiliencia Operativa Digital para el sector financiero.



CÓDIGO DE RED NCCS

Normas específicas del sector para los aspectos de ciberseguridad de las redes transfronterizas, flujos de electricidad.



PARTE-IS (PARTE-IS10)

Normas de seguridad de la información para el subsector del transporte aéreo.



Un marco coherente y complementario que refuerza la ciberseguridad, la resiliencia y la cooperación en toda la Unión Europea.



DIRECTIVA NIS2

CUERPO LEGAL COMPLETO

El marco legal de la Directiva NIS2 se compone de tres niveles complementarios que, en conjunto, conforman el **cuerpo completo legal**.



1

DIRECTIVA (UE) 2022/2555 NIS2



Establece los objetivos, las obligaciones esenciales y el marco de ciberseguridad que deben aplicar los Estados miembros.



Define **QUÉ** debe lograrse (resultado a alcanzar)

2

REGLAMENTOS DE EJECUCIÓN



Desarrollan aspectos técnicos y procedimentales de la NIS2. Son adoptados por la Comisión Europea.



Especifican **CÓMO** debe aplicarse (requisitos técnicos y procedimientos)

3

GUÍAS DE IMPLEMENTACIÓN DE LOS REGLAMENTOS



Emitidas por ENISA u otros organismos competentes. Proporcionan recomendaciones y buenas prácticas para una aplicación armonizada.



Orientan y apoyan la aplicación uniforme y efectiva



CUERPO COMPLETO LEGAL NIS2

Directiva NIS2 + Reglamentos de Ejecución + Guías de Implementación
Marco jurídico completo para una ciberseguridad elevada y armonizada en la UE.



SITUACIÓN EN ESPAÑA

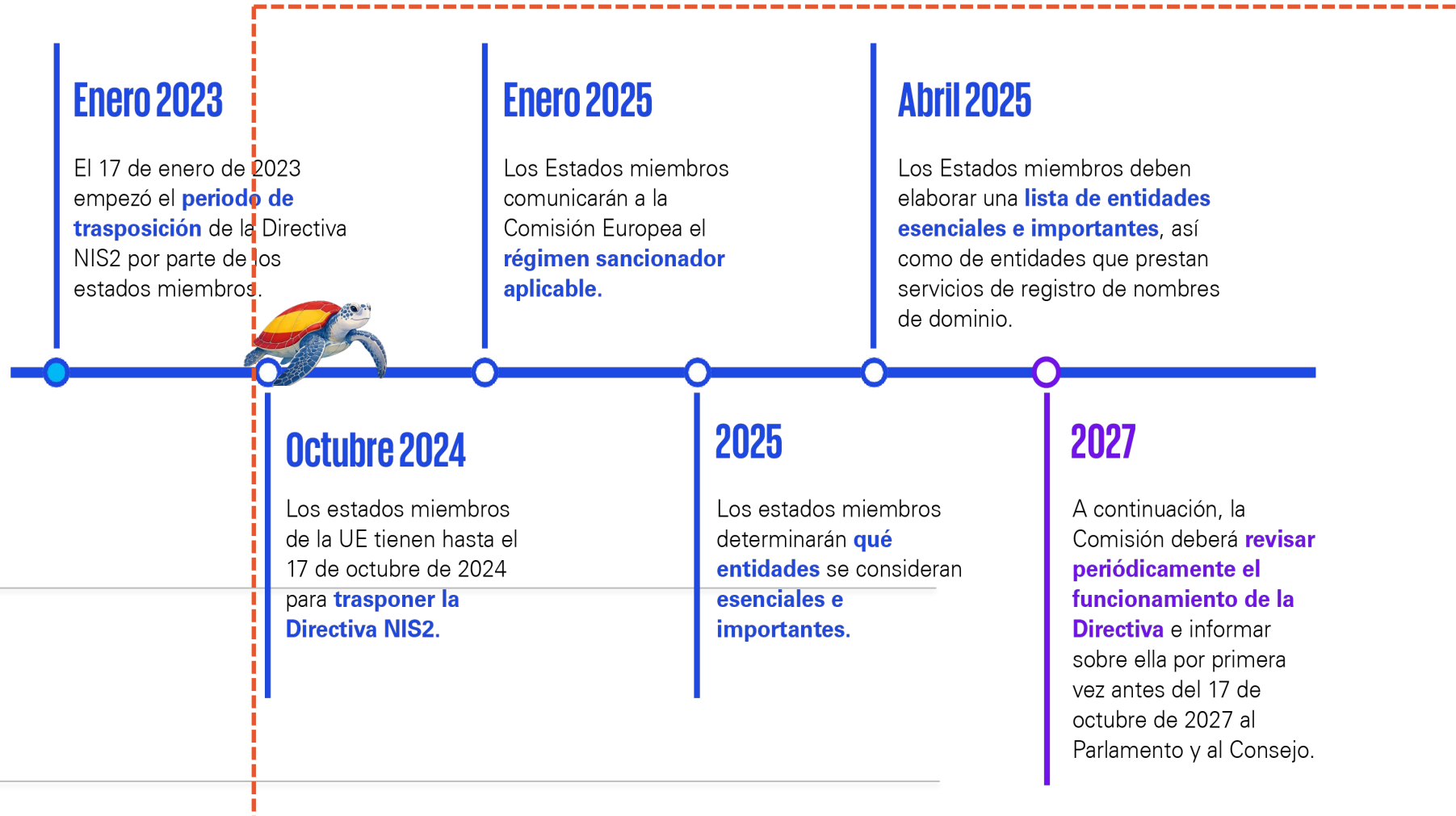
La trasposición de la Directiva NIS2 al ordenamiento jurídico español se encuentra actualmente en fase de **ANTEPROYECTO DE LEY**.



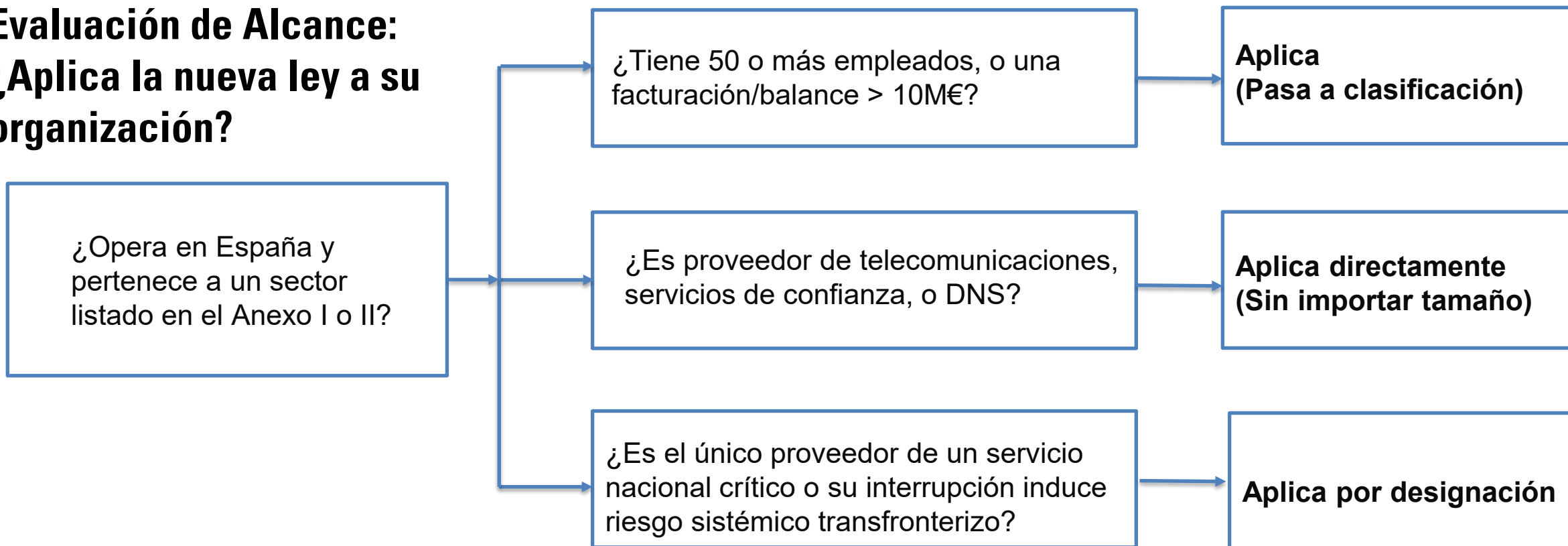
EN TRAMITACIÓN
ANTEPROYECTO DE LEY

Situación

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión



Evaluación de Alcance: ¿Aplica la nueva ley a su organización?



Exclusiones: Entidades dedicadas exclusivamente a seguridad nacional, defensa, Cortes Generales, Banco de España o sector financiero regulado por DORA.

La frontera normativa: Criterios para Entidades Esenciales e Importantes

	Entidades Esenciales	Entidades Importantes
Criterio de Tamaño	Grandes empresas (>250 empleados o >50M€ facturación y >43M€ balance).	Medianas empresas (>50 empleados o >10M€ facturación).
Sectores Afectados	Sectores del Anexo I (Energía, Transporte, Banca, Salud, Infraestructura Digital).	Resto de entidades del Anexo I y todo el Anexo II (Postal, Residuos, Alimentación, Fabricación).
Inclusiones Especiales	Proveedores DNS, dominios TLD, servicios de confianza, telecos medianas.	Entidades no catalogadas explícitamente como esenciales.
Enfoque de Supervisión	Supervisión a priori (Proactiva y continua).	Supervisión a posteriori (Reactiva, basada en indicios).

ÁMBITO SECTORIAL: DE NIS A NIS2

Comparación de las Directivas (UE) 2016/1148 y 2022/2555

ANEXO I · SECTORES DE ALTA CRITICIDAD

El anexo no determina por sí solo la condición de entidad esencial

1

Energía

AMPLIADO

NIS y NIS2: electricidad · petróleo · gas
NIS2 añade: hidrógeno · calefacción y refrigeración urbanas

2

Transportes

Aéreo · ferrocarril · marítimo y fluvial · carretera

3

Banca

4

Infraestructuras de mercados financieros

5

Sector sanitario

AMPLIADO

Ámbito ampliado por NIS2

6

Agua potable

7

Aguas residuales

8

Infraestructura digital

AMPLIADO

NIS y NIS2: IXP · DNS · TLD · nube
NIS2 añade: centros de datos · CDN · confianza · comunicaciones electrónicas

9

Gestión de servicios TIC

MSP · MSSP

10

Administración pública

Central y regional; nivel local según extensión nacional

11

Espacio

Infraestructuras terrestres

*

Industria nuclear

Sector adicional del marco español

ANEXO II · OTROS SECTORES CRÍTICOS

Con carácter general, entidades importantes; existen excepciones del artículo 3

1

Servicios postales y de mensajería

2

Gestión de residuos

3

Sustancias y mezclas químicas

Fabricación · producción · distribución

4

Alimentación

Distribución mayorista y producción y transformación industriales de alimentos

5

Fabricación

· Productos sanitarios
· Productos informáticos, electrónicos y ópticos
· Material eléctrico
· Maquinaria y equipo
· Vehículos de motor y remolques
· Otro material de transporte

6

Proveedores digitales

AMPLIADO

NIS y NIS2: mercados en línea · buscadores
NIS2 añade: plataformas de redes sociales
La nube pasa al Anexo I

7

Investigación

Organizaciones de investigación

CÓDIGO CROMÁTICO  Ya incluido en NIS y mantenido en NIS2  Incorporado por NIS2  Ya incluido, con alcance ampliado o reordenado En la NIS2  Adicional del marco español al trasponer la NIS

Nota: los anexos identifican sectores y tipos de entidad. La clasificación como entidad esencial o importante depende de los criterios del artículo 3 de NIS2.

Fuente: Directivas (UE) 2016/1148 y 2022/2555; marco español: RDL 12/2018 y Ley 8/2011.



XUNTA
DE GALICIA



CENTRO DE NOVAS TECNOLOXÍAS
DE GALICIA

SERVICIO ESENCIAL DE LA UE (NIS2)

DISTRIBUCIÓN DE AGUA POTABLE

PROCESOS DE NEGOCIO (Servicio Esencial)

Captación y
Potabilización



Distribución y
Suministro



Atención al
ciudadano



Mantenimiento de
infraestructuras



Calidad del agua
y medioambiente



El agua llega al ciudadano de forma segura, continua y de calidad

PROCESOS DE SISTEMAS DE INFORMACIÓN (OT + IT)

GESTIÓN DE CLIENTES

- Altas / Bajas de contrato
- Facturación
- Lectura de contadores
- Atención de incidencias

GESTIÓN OPERATIVA (SCADA)

- Monitorización de la red
- Control de bombas y válvulas
- Gestión de alarmas
- Calidad del agua en tiempo real

MANTENIMIENTO

- Planificación de trabajos
- Gestión de activos
- Órdenes de trabajo
- Inventario y almacén

SOPORTE CORPORATIVO

- RRHH
- Finanzas
- Compras
- Jurídico
- Comunicación

SISTEMAS DE INFORMACIÓN (IT / OT)

SISTEMAS OT (SCADA)

- PLCs / RTUs
- HMI / SCADA
- Históricos

SISTEMAS EMPRESARIALES (IT)

- SAP
- Billing
- GIS
- BD

OTROS SISTEMAS

- Gestión documental
- Correo / Colaboración
- Backup

INFRAESTRUCTURA Y DATOS

INFRAESTRUCTURA

- Servidores
- Almacenamiento
- Redes
- Virtualización
- Cloud privado

DATOS (INFORMACIÓN CRÍTICA)

- Datos de operación en tiempo real (caudales, niveles, presiones, calidad)
- Datos de clientes y facturación
- Planos e información de la red
- Registros de mantenimiento y activos
- Logs de seguridad y auditoría



RESULTADO



Servicio de agua seguro,
continuo y resiliente

- ✓ Disponibilidad
- ✓ Integridad
- ✓ Confidencialidad
- ✓ Trazabilidad
- ✓ Cumplimiento NIS2

USUARIOS / CLIENTES

Ciudadanos, empresas,
administraciones públicas

ENTORNO FÍSICO (OT)

- Captaciones
- Plantas potabilizadoras
- Depósitos
- Estaciones de bombeo
- Red de distribución
- Contadores inteligentes

MADUREZ Y CAMINO DE ADOPCIÓN DE LA NIS2

Cuanto mayor es la madurez de la organización, más sencillo será el camino hacia el cumplimiento de la NIS2.



Invertir en madurez de ciberseguridad no solo facilita el cumplimiento de la NIS2, sino que fortalece la resiliencia y confianza de la organización.



Obligaciones normativas y estructura de cumplimiento

Resumen ejecutivo de las obligaciones NIS2/APL

La Directiva NIS2 y su transposición española (APL) establecen un marco regulador integral que obliga a las entidades esenciales e importantes a implementar:

Medidas técnicas y organizativas de gestión de riesgos, utilizando el ENS como referente en España, y a cumplir con un flujo estricto de notificación de incidentes significativos (24h/72h/1 mes).

Las organizaciones deben designar un Responsable de la Seguridad de la Información (RSI) con garantías de independencia, mientras que la alta dirección asume responsabilidad personal y subsidiaria, enfrentando sanciones de hasta 10 millones de euros o el 2% de la facturación mundial en caso de negligencia.

Obligaciones de NIS2

La Directiva NIS2 exige medidas técnicas, operativas y organizativas, proporcionadas, para gestionar riesgos y minimizar incidentes de ciberseguridad, en los sectores que proporcionan servicios de alta criticidad y sectores críticos.

Adaptación en APL español

El APL añade concreciones nacionales y criterios del Centro Nacional de Ciberseguridad para medidas y certificaciones.

Cumplimiento y certificación

Las entidades deben demostrar cumplimiento a través de certificación, evaluación o auditoría según su clasificación.

Enfoque práctico para CISOs, responsables y Órganos de Dirección.

Programa integrado de gobierno

NIS2/APL debe abordarse como un programa integral de gobierno que incluye riesgos, resiliencia y evidencia.

Si la entidad está sujeta a otras obligaciones como el ENS, debe incorporar en su programa los aspectos que refuercen el cumplimiento de ambas legislaciones.

Controles basados en riesgos

Los controles deben estar proporcionados al nivel de riesgo y estar aprobados para asegurar la efectividad.

Medición y revisión continua

Es esencial medir, revisar y conectar los controles con decisiones de negocio para asegurar la mejora continua.

DECISIONES INFORMADAS !!

Comparativa entre NIS2 y APL española

Lectura jurídica mínima y diferencias clave

Esta forma de referirnos a la NIS2 y a su trasposición, que todavía está en fase de Ante Proyecto de Ley (APL) no debe llevarnos a equívocos: **No** son dos leyes diferentes. Las Directivas requieren de trasposiciones nacionales al Ordenamiento Jurídico de cada uno de los estados miembros.

Contenido jurídico de NIS2

NIS2 establece requisitos mínimos para seguridad cibernética en servicios esenciales.

Aportaciones del APL

Las Directivas requieren de trasposición.

El APL añade disposiciones específicas que amplían y complementan los requisitos de NIS2.

Diferencias clave

Las diferencias entre NIS2 y APL radican en la concreción, de Gobierno (Estado) y operativa y en las obligaciones específicas para los sectores regulados.

Diferencias y su aplicación práctica

Comparación normativa NIS2 y APL

APL = NIS2 + refuerzos o concreciones para el ámbito nacional ;**por ejemplo, la figura del RSI, el Centro Nacional de Ciberseguridad, los CSIRTs de referencia o las autoridades de control y puntos de contacto sectoriales.**

Gestión de riesgos y cadena de suministro

Se enfatiza la gestión formal de riesgos en la cadena de suministro. **La APL añade punto de contacto de seguridad principal** para cada proveedor y perfiles con enfoque incremental.

Demostración de cumplimiento

NIS2 exige cumplimiento supervisable , APL exige demostrar cumplimiento;; esenciales con certificación de conformidad e importantes con certificación o evaluación/auditoría

Uso de estándares y ENS. Base técnica.

NIS2: Normas europeas e internacionales pertinentes

APL: ENS como base; estándares europeos o internacionales equivalentes mediante reconocimiento.

Se propone usar ENS base, integrando ISO/IEC 27001/27002

Gobernanza Institucional

El APL concreta la autoridad mediante la creación del **Centro Nacional de Ciberseguridad (CNC)** como autoridad única, y distribuye la supervisión sectorial entre los Ministerios de **Defensa, Interior y Transformación Digital**, algo que la Directiva deja a discreción del Estado

Instrumentos de Cumplimiento

El APL introduce la obligación técnica de elaborar y suscribir una **Declaración de Aplicabilidad (SoA)**, vinculada al artículo 28 del ENS, para mapear las medidas sobre los activos, un documento que no aparece con ese nivel de detalle en la Directiv

Plataformas Operativas:

La normativa española concreta el uso de la **Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes** para canalizar todas las notificaciones obligatorias, centralizando la **respuesta técnica en CSIRTs específicos (CCN-CERT, INCIBE-CERT y ESPDEF-CERT)** según el sector

Obligaciones Sectoriales Específicas

El APL permite la aprobación de **perfiles específicos de cumplimiento** de carácter incremental para determinados sectores o tipos de operadores, permitiendo ajustar la ley a la criticidad y realidad de cada industria de forma más detallada que el texto europe (PCE).

Método de implantación en 12 pasos

Pasos 1 y 2: Determinación de aplicabilidad y clasificación

Determinación si la entidad está en el Ámbito

Identificar sectores, servicios prestados, tamaño y criticidad para confirmar si la entidad entra en el alcance regulatorio.

Clasificar la Entidad y los servicios regulados

Determinar si la entidad será esencial o importante y qué servicios concretos quedan bajo el perímetro. Resultado: matriz de servicios regulados, responsables, sistemas soporte y dependencias externas



Pasos 3 a 5: Gobierno, gestión de riesgos e inventario



Modelo de Gobierno Ciberseguridad

Crear y aprobar un modelo formal de gobierno con comité, roles clave y relaciones interdepartamentales; constituir o adaptar comité de ciberseguridad, asignar **RSI/CISO**, definir RACI, relación con DPO, continuidad, compras, jurídico, SOC y CSIRT. Resultado: modelo de gobierno formalmente aprobado.



XUNTA
DE GALICIA

Aprobar apetito y Metodología de Gestión de Riesgos

Definir nivel de apetito, metodología y criterios claros para análisis, tratamiento, aceptación y escalado de riesgos en la organización.

Inventario de Activos, servicios y dependencias

Mantener un inventario de activos tecnológicos, datos, procesos, servicios críticos, dependencias de proveedores, conectividades, identidades privilegiadas, nube, OT/IoT si aplica y riesgos asociados. Resultado: CMDB o inventario vivo con “propietarios internos”, criticidad y exposición. Mapa de riesgos

PASOS 6 A 8: GAP ASSESSMENT, SoA E IMPLANTACIÓN

Gap assessment

Evaluar 10 bloques mínimos frente a art. 21, art. 19, ENS e ISO 27002 aprobar un modelo formal de gobierno con comité, roles clave y relaciones interdepartamentales

Declaración NIS2/APL

Definir controles aplicables, alcance, excepciones, compensatorios, responsables y evidencias

Implantar controles

Activar capacidades técnicas, operativas y organizativas en seguridad IoT si aplica.
Resultado: SOA

PASOS 9 A 12: INDUSTRIALIZACIÓN DE INCIDENTES, EXPEDIENTE DE EVIDENCIAS Y ASEGURAMIENTO

9. Industrializar la gestión de incidentes: Procedimientos de detección, clasificación, escalado, contención, notificación, coordinación con legal/DPO, preservación de evidencias, comunicación y recuperación. Resultado: playbooks y ejercicios de simulación.

10. Construir el expediente de evidencias: Repositorio con políticas, actas, métricas, informes, pruebas, registros, decisiones, riesgos aceptados, revisiones de proveedores, simulacros, auditorías y acciones correctivas. Resultado: audit pack vivo.

11. Preparar certificación, auditoría o evaluación: Para esenciales, preparar certificación de conformidad. Para importantes, decidir certificación o evaluación/auditoría de postura de seguridad. Resultado: plan de aseguramiento y calendario.

12. Mantener mejora continua y reporting ejecutivo Revisiones periódicas, KRIs/KPIs, reporting al Consejo, lecciones aprendidas, revisión de riesgos y actualización ante cambios regulatorios o tecnológicos. Resultado: ciclo anual NIS2 integrado en gobierno corporativo.

Desarrollo operativo de los
artículos 21 NIS2 y 19 APL

Implantación práctica de los bloques normativos y evidencias mínimas

Marco Integral de Seguridad

El marco se basa en los artículos 21 y 19, alineado con ENS e ISO/IEC 27002 para asegurar gestión efectiva.

Bloques Temáticos Clave

Se abordan desde políticas, análisis de riesgos, hasta ciberhigiene, criptografía y control de acceso.

Evidencias y Auditoría

Se detallan evidencias mínimas para facilitar implantación práctica y auditorías de cumplimiento.

Mejora Continua y Cumplimiento

Evaluación continua mediante auditorías y métricas garantiza la mejora y alineación con estándares.

Bloque art. 21/art. 19	Implantación práctica	Evidencias mínimas	Referencias ENS / ISO 27002
a) Políticas de seguridad y análisis de riesgos	Política de seguridad aprobada; metodología de análisis de riesgos; inventario de activos; criterios de aceptación de riesgo; matriz de riesgos por servicio regulado.	Acta de aprobación; política; metodología; inventario; informe de riesgos; plan de tratamiento; riesgos residuales aceptados.	ENS: org.1, op.pl, op.exp, op.risk, mp.info. ISO/IEC 27002:2022: 5.1, 5.2, 5.4, 5.9, 5.36.
b) Gestión de incidentes	Modelo SOC/CSIRT; taxonomía de incidentes; playbooks; preservación de evidencias; escalado; coordinación con DPO y jurídico; criterios de notificación.	Procedimiento; matriz de severidad; tickets; informes post-incidente; actas de crisis; cadena de custodia; simulacros.	ENS: op.exp, op.mon, op.cont, op.ext. ISO/IEC 27002:2022: 5.24, 5.25, 5.26, 5.27, 5.28.
c) Continuidad, backup, recuperación y crisis	BIA; RTO/RPO; plan de continuidad; backup 3-2-1 o equivalente; recuperación ante desastre; gestión de crisis; pruebas periódicas.	BIA; planes; evidencias de backup; pruebas de restauración; resultados de simulacros; acciones correctivas.	ENS: op.cont, mp.info, mp.si. ISO/IEC 27002:2022: 5.29, 5.30, 8.13, 8.14.
d) Seguridad de cadena de suministro	Clasificación de proveedores; requisitos contractuales; evaluación inicial y continua; punto de contacto de seguridad; derecho de auditoría; gestión de incidentes de proveedor.	Inventario de proveedores; cuestionarios; cláusulas; SLAs; evaluaciones; rating externo si aplica; actas de revisión.	ENS: op.ext, op.nub, org.4. ISO/IEC 27002:2022: 5.19, 5.20, 5.21, 5.22, 5.23.
e) Seguridad en adquisición, desarrollo y mantenimiento; vulnerabilidades	SSDLC; requisitos de seguridad en proyectos; SAST/DAST; revisión de arquitectura; patch management; divulgación coordinada de vulnerabilidades; SBOM cuando aplique.	Requisitos en pliegos; threat models; informes de pruebas; registros de cambios; backlog de vulnerabilidades; SLA de parcheo; SBOM.	ENS: op.exp, op.mon, mp.sw, mp.si, op.ext. ISO/IEC 27002:2022: 5.8, 8.8, 8.9, 8.25, 8.26, 8.27, 8.28, 8.32.
f) Evaluación de eficacia de medidas	Programa de control interno; métricas; auditorías; pruebas técnicas; revisión de KRIs/KPIs; revisión por dirección; red teaming/purple teaming según riesgo.	Cuadro de mando; informes de auditoría; resultados pentest; planes de remediación; actas de revisión; métricas históricas.	ENS: art. 31 auditoría, art. 37 control, anexo II op.mon. ISO/IEC 27002:2022: 5.35, 5.36, 8.16, 8.34.
g) Ciberhigiene y formación	Programa de concienciación; formación por rol; formación a dirección; campañas phishing; seguridad en uso de credenciales; higiene endpoint.	Plan de formación; asistencia; contenidos; evaluación; campañas; métricas de mejora.	ENS: art. 15, org.2, mp.per. ISO/IEC 27002:2022: 6.3, 6.4, 8.1, 8.7.
h) Criptografía y cifrado	Política criptográfica; cifrado en tránsito y reposo; gestión de claves; protección de secretos; algoritmos aprobados; revisión post-cuántica progresiva.	Política; inventario de certificados; configuración TLS; HSM/KMS; rotación de claves; auditoría de acceso a claves.	ENS: mp.com, mp.info, mp.si. ISO/IEC 27002:2022: 8.24, 5.14.
i) Seguridad RRHH, control de acceso y activos	Screening proporcional; altas/bajas/cambios; mínimo privilegio; PAM; IAM; revisiones de permisos; inventario; segregación de funciones.	Procedimientos RRHH; registros de altas/bajas; informes IAM/PAM; recertificaciones; inventario; SoD.	ENS: mp.per, op.acc, mp.info. ISO/IEC 27002:2022: 5.9, 5.15, 5.16, 5.17, 5.18, 6.1, 6.5.
j) MFA/autenticación continua y comunicaciones seguras	MFA en accesos críticos y remotos; autenticación adaptativa; comunicaciones seguras; canales de emergencia; endurecimiento de correo y colaboración.	Política MFA; evidencias IAM; configuración VPN/ZTNA; pruebas de comunicaciones de crisis; registros de acceso.	ENS: op.acc, mp.com, op.exp. ISO/IEC 27002:2022: 5.16, 5.17, 8.5, 8.20, 8.21.

Paquetes implantables
para cumplir NIS2/APL

Gobierno y accountability

Entregables Clave

Incluyen política de seguridad, modelo de gobierno, RACI, comité, reporting y formación directiva.

Estructura de Gobierno

El modelo incluye comité y reporting directo al Consejo para asegurar accountability.

Indicadores de Rendimiento

Siguen y registran: reuniones, decisiones de riesgo, aceptación de riesgos y cumplimiento del plan.

Gestión de riesgos

Componentes clave

Incluye metodología, inventario, análisis de impacto empresarial y matriz de riesgos para gestionar amenazas.
Desviaciones.

Tratamiento y seguimiento

Aborda tratamiento de riesgos, riesgos residuales y excepciones para asegurar control constante.

Indicadores de rendimiento

Mide activos críticos con riesgo actualizado y porcentaje de medidas vencidas para mejora continua.

Gestión de incidentes. Operación SOC/CSIRT

Entregables Clave

Incluyen
Procedimientos,
taxonomía, esclados,
playbooks,
herramientas
SIEM/SOAR y matriz de
severidad para una
gestión estructurada.

Si la entidad dispone
tanto de un CSIRT como
de un SOC, las
responsabilidades y
matriz RACI deben ser
claras. .

Procedimientos y SLA

Procedimientos de
Gestión escalado y
comunicación (interna y
externa),
Implementación de
guardias, acuerdos SLA
y procedimientos de
notificación para
respuesta eficiente.
Activación DFIR y/o
Ciberseguro. Relación
con grupos de soporte y
POC de terceros

Indicadores de Desempeño

Monitorización de
MTTD, MTTR, tiempo
de escalado, incidentes
y tasa de falsos
positivos para mejorar
operaciones.

Resiliencia y continuidad



Entregables claves

Incluyen análisis de impacto al negocio, plan de recuperación ante desastres, Plan de Continuidad de Negocio y pruebas de restauración para asegurar continuidad.

Procedimientos claros de escalado a crisis y continuidad.

Gestión de crisis y backups

La gestión de crisis y el backup seguro/inmutable protegen contra pérdidas de datos y ataques ransomware.

Indicadores de desempeño

Se miden cumplimiento de RTO/RPO, éxito de restauraciones y antigüedad de pruebas para garantizar resiliencia.

Terceros



Entregables clave

Incluyen inventario, clasificación, cuestionario, cláusulas, SLAs, Penalizaciones, POC de seguridad y evaluación continua para gestionar terceros.

Derecho de auditoría

Garantiza el derecho a auditar proveedores para mantener la seguridad y cumplimiento normativo.

Indicadores de desempeño

Miden proveedores críticos evaluados, contratos con cláusula NIS2, proveedores sin POC e incidentes relacionados con terceros.

Tecnología base

Entregables clave

Incluyen: Adquisición segura, hardening, EDR, gestión de vulnerabilidades, patching, MFA, IAM/PAM, cifrado y segmentación para seguridad básica (entre otras).

Importancia de tecnología base

La tecnología base garantiza una defensa sólida y control sobre la infraestructura TI para prevenir amenazas.

Indicadores de seguridad

Miden exposición crítica, vulnerabilidades sin tratar, cobertura MFA, control de cuentas privilegiadas y activos desconocidos.

Evidencia y aseguramiento

Entregables claves

Incluye expediente NIS2, auditorías, certificaciones, pruebas, actas, KPIs/KRIs y declaración de aplicabilidad como entregables esenciales.

Indicadores de control

Monitorea evidencias caducadas, hallazgos abiertos, controles sin responsable y controles sin pruebas para asegurar cumplimiento.

Roadmap de implantación y checklist de adopción

Roadmap de 12 meses para la implantación

(Ejemplo propuesta)

PERIODO	ACTUACIONES
Mes 0-1	Aplicabilidad, sponsor, gobierno, perímetro, clasificación preliminar esencial/importante.
Mes 1-2	Inventario regulado, mapa de servicios, activos, terceros y procesos críticos.
Mes 2-3	Gap assessment contra art. 21/art. 19, ENS e ISO 27002. Priorización por riesgo.
Mes 3-4	Aprobación de política, metodología de riesgo, RACI, comité, reporting al Consejo.
Mes 4-6	Implantación acelerada de quick wins: MFA, backup, vulnerabilidades, incidentes, terceros críticos.
Mes 6-8	Industrialización SOC/CSIRT, playbooks, notificación, crisis, continuidad y simulacros.
Mes 8-10	Declaración de aplicabilidad, expediente de evidencias, auditoría interna, remediación.
Mes 10-12	Certificación/evaluación, presentación a dirección, plan anual y mejora continua.

Checklist CISO de adopción práctica

Marco de Control de Seguridad

El checklist ofrece un marco para gestionar seguridad y cumplimiento, alineado con normativas NIS2 y APL.

Áreas Clave Evaluadas

Se cubren gobierno, riesgos, incidentes, proveedores, continuidad, identidades, vulnerabilidades y aseguramiento.

Preguntas de Control Específicas

Cada área incluye preguntas para verificar procesos, responsables, evidencias y seguimiento efectivo.

Formalización y Mejora Continua

El enfoque asegura formalización, trazabilidad y periodicidad, fomentando la mejora continua en seguridad.

EJEMPLO

Área	Preguntas de control
Gobierno	¿Existe aprobación formal del marco NIS2/APL por dirección? ¿Hay RACI? ¿Hay reporting al Consejo?
Riesgos	¿Están identificados servicios regulados, activos y dependencias? ¿Hay riesgos residuales formalmente aceptados?
Controles	¿Cada bloque del art. 21/art. 19 tiene controles, owner, periodicidad y evidencia?
Incidentes	¿Hay criterios de incidente significativo, playbooks, escalado y canal de notificación?
Terceros	¿Todos los proveedores críticos tienen evaluación, cláusulas y punto de contacto de seguridad?
Continuidad	¿Se han probado backup, restauración, crisis y DR?
Identidades	¿MFA, PAM, revisiones de acceso y bajas están controladas?
Vulnerabilidades	¿Existe SLA por criticidad y seguimiento ejecutivo de vulnerabilidades críticas?
Evidencias	¿Existe repositorio auditable con trazabilidad de decisiones y pruebas?
Aseguramiento	¿Está planificada certificación, auditoría o evaluación según clasificación?

Cuadro de mando y errores habituales en la implantación

MÉTRICA	CONTENIDO	LECTURA EJECUTIVA
Riesgo residual	Número de riesgos altos/muy altos aceptados o sin tratamiento	Debe mostrar qué riesgo asume el negocio.
Incidentes	Incidentes significativos, MTTD, MTTR, escalados regulatorios	Debe conectar operación con impacto en servicio.
Continuidad	Cumplimiento RTO/RPO y pruebas de restauración	Debe evidenciar resiliencia, no solo backup.
Terceros	Porcentaje de proveedores críticos evaluados y con cláusulas NIS2	Debe visualizar riesgo extendido.
Vulnerabilidades	Críticas vencidas, tiempo medio de remediación, exposición externa	Debe priorizar por explotabilidad e impacto.
Identidades	Cobertura MFA/PAM y cuentas privilegiadas revisadas	Debe mostrar reducción de superficie de ataque.
Cumplimiento	Estado de certificación/auditoría, hallazgos abiertos, plan de remediación	Debe anticipar supervisión.

Errores habituales

Pensar que sólo es para empresas grandes.

No sólo es una orientación al cumplimiento, sino hacia el desastre causado por un incidente crítico.

Gestión incorrecta de NIS2

Tratar NIS2 solo como documentación limita su eficacia como modelo operativo supervisable.

Qué los Órganos de Dirección no lideren el proceso, es la mayor dificultad.

**Incorrecta Gestión de incidentes.
Confusión entre SOC y CSIRT**

Una gestión de incidentes orientada exclusivamente a la rápida recuperación, sin evidencias, sin análisis profundo, sin lesiones aprendidas: es un error.

En Organizaciones grandes, no distinguir SOC operativo de la función CSIRT puede afectar la gestión integral de incidentes.

Falta de pruebas y evidencias

No probar restauración ni comunicación de crisis y ausencia de evidencias trazables comprometen la seguridad.

Omisión de actores clave

Olvidar proveedores críticos y no integrar jurídico o DPO en incidentes con impacto en datos personales es un error crítico.

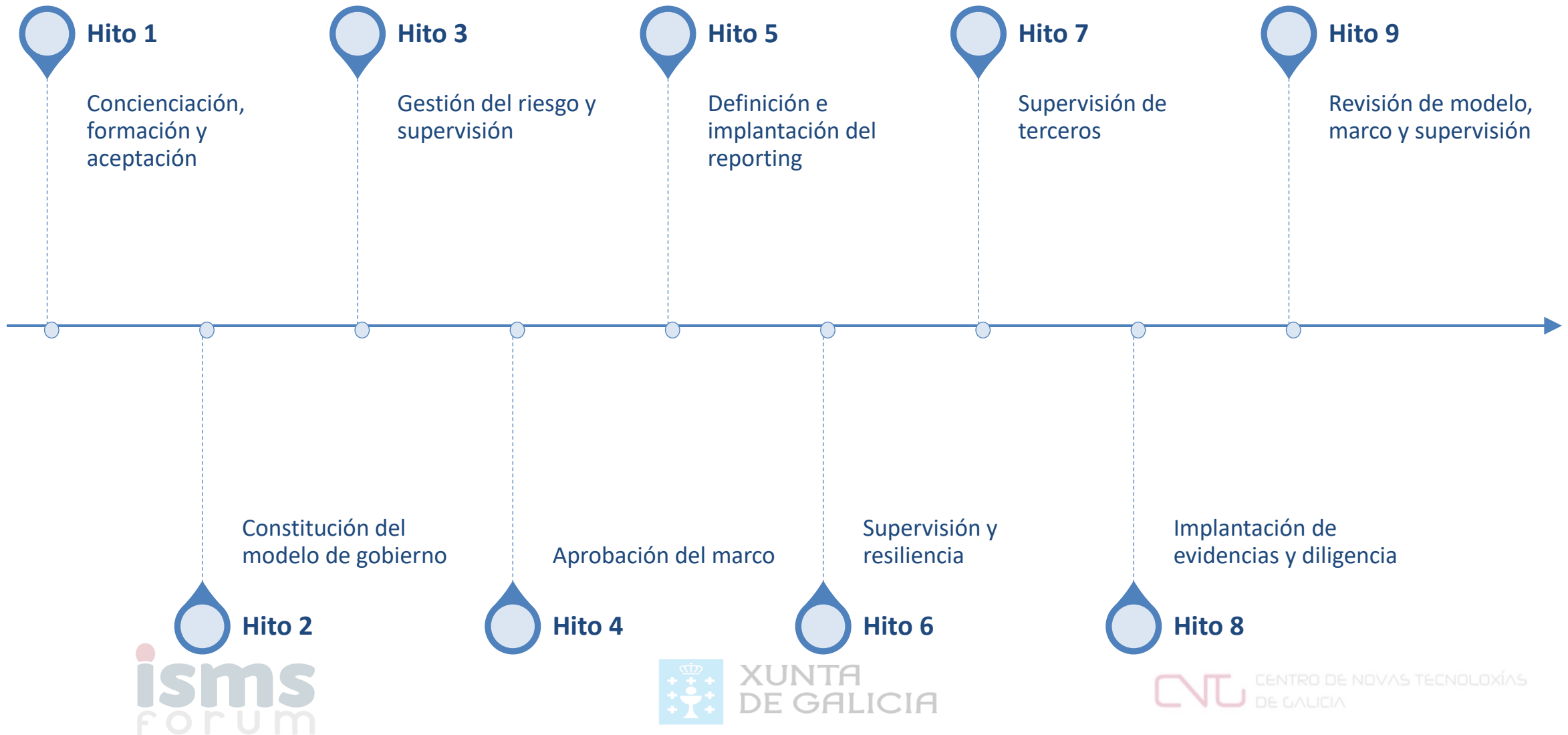
Subestimar o ignorar el control de la cadena de Suministro

Todos los aspectos de control están, en principio, bajo su responsabilidad directa de ejecución; salvo la cadena de suministro y las obligaciones de los Órganos de Control.

EJEMPLO de Paquete de asunción
responsabilidad órganos de dirección

Órganos de gobierno

Hitos clave de adopción



PAQUETE DE ADOPCIÓN DE RESPONSABILIDADES

Este paquete define las actuaciones mínimas de gobierno, supervisión, formación y evidencia que permiten al órgano de dirección asumir formalmente sus responsabilidades en materia de ciberseguridad, en línea con las exigencias de NIS2 sobre aprobación, supervisión y capacitación periódica del Órgano de Gobierno, y con un enfoque coherente con otros marcos como ENS, ISO 27001 y protección de datos.

Fase 1. Concienciación y aceptación formal de responsabilidades

Fase 2. Constitución del modelo de gobierno

Fase 3. Gestión del riesgo y supervisión

Fase 4. Marco normativo y control

Fase 5. Supervisión y reporting

Fase 6. Supervisión de resiliencia y respuesta

Fase 7. Supervisión de terceros

Fase 8. Evidencia regulatoria y diligencia debida

FASE 1

CONCIENCIACIÓN Y ACEPTACIÓN FORMAL DE RESPONSABILIDADES

1.2 Formación obligatoria de Alta Dirección

Cumplir la obligación legal de capacitación periódica del órgano de dirección. Proporcionada. para gestionar riesgos y minimizar incidentes de ciberseguridad, en los sectores que proporcionan servicios de alta criticidad y sectores críticos.

1.1 Sesión ejecutiva de sensibilización NIS2

Objetivo: Explicar al órgano de dirección las obligaciones derivadas de NIS2, el régimen sancionador, la posible responsabilidad personal o solidaria, el impacto reputacional del incumplimiento y la exigencia de aprobar, supervisar y comprender las medidas de gestión del riesgo.

Contenido recomendado: NIS2 y su impacto en el Consejo; alcance y aplicabilidad; responsabilidades personales; riesgos de incumplimiento; precedentes regulatorios; relación con DORA, ENS, ISO 27001 y protección de datos.

Entregables: Acta del Consejo con declaración de conocimiento y evidencia de asistencia.

Temáticas mínimas

Gestión de riesgos, amenazas actuales, resiliencia y gestión de crisis..

Recomendación

Formación anual obligatoria para la Alta Dirección.

FASE 2

CONSTITUCIÓN DEL MODELO DE GOBIERNO

2.2 Designación formal del CISO

Nombramiento formal del responsable de seguridad.

Recomendación

Reuniones mensuales y reporting trimestral al Consejo. **Centro Nacional de Ciberseguridad (CNC)** como autoridad única, y distribuye la supervisión sectorial entre los Ministerios de **Defensa, Interior y Transformación Digital**, algo que la Directiva deja a discreción del Estado

2.1 Aprobación formal del modelo

El órgano de dirección debe aprobar formalmente el modelo de gobierno. **por ejemplo, la figura del RSI, el Centro Nacional de Ciberseguridad, los CSIRTs de referencia o las autoridades de control y puntos de contacto sectoriales.**

2.3 Constitución del Comité de Seguridad

Órgano de seguimiento y supervisión del marco NIS2. **Declaración de Aplicabilidad (SoA)**, vinculada al artículo 28 del ENS, para mapear las medidas sobre los activos, un documento que no aparece con ese nivel de detalle en la Directiv

Alcance mínimo

Roles y responsabilidades, segregación de funciones y líneas de reporte. **La APL añade punto de contacto de seguridad** principal para cada proveedor y perfiles con enfoque incremental.

Participantes recomendados

CISO, CIO, Riesgos, Compliance, Legal y Operaciones. **Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes** para canalizar todas las notificaciones obligatorias, centralizando la **respuesta técnica en CSIRTs específicos (CCN-CERT, INCIBE-CERT y ESPDEF-CERT)** según el sector

Coherencia NIS2

Alineado con la supervisión de medidas de gestión del riesgo exigida por NIS2. exige cumplimiento supervisable, APL exige demostrar cumplimiento; esenciales con certificación de conformidad e importantes con certificación o evaluación/auditoría

Funciones

Seguimiento del riesgo, del plan NIS2 y de incidentes. **perfiles específicos de cumplimiento** de carácter incremental para determinados sectores o tipos de operadores, permitiendo ajustar la ley a la criticidad y realidad de cada industria de forma más detallada que el texto europe (PCE)

Priorización de inversiones, supervisión de terceros y seguimiento regulatorio.

FASE 3

GESTIÓN DEL RIESGO Y SUPERVISIÓN

3.1 Aprobación del apetito de riesgo de ciberseguridad

El Consejo aprueba niveles de riesgo aceptable, criticidad, tolerancia a interrupciones y riesgos no aceptables. Aprobar un modelo formal de gobierno con comité, roles clave y relaciones

interdepartamentales; constituir o adaptar comité de ciberseguridad, asignar RSI/CISO, definir RACI, relación con DPO, continuidad, compras, jurídico, SOC y CSIRT. Resultado: modelo de gobierno formalmente aprobado.

3.2 Aprobación de la metodología de gestión de riesgos

Debe contemplar: identificación, valoración, tratamiento, seguimiento y reevaluación continua.

3.3 Supervisión periódica del mapa de riesgos

La Alta Dirección debe recibir información periódica y accionable para una supervisión real y documentada.

¿IoT si aplica?.

Resultado: Mapa de riesgos

FASE 4

aprobación del marco

4.1 Aprobación del Marco Normativo.

Definición y aprobación de las políticas mínimas de ciberseguridad.

Política de seguridad; Gestión de incidentes; Gestión de accesos; Gestión de vulnerabilidades; Backup y recuperación; Seguridad cloud; Seguridad de terceros; Gestión de identidades; Continuidad de negocio; Gestión de crisis; Desarrollo seguro; Clasificación de información

4.2 Aprobación del plan director de ciberseguridad / roadmap NIS2

Aprobación del plan de despliegue y priorización.

Diagnóstico GAP;
Priorización; Inversiones;
Quick wins; Dependencias;
Roadmap plurianual

4.3 Aprobación del presupuesto de ciberseguridad

Tecnología; Servicios SOC; CSIRT; Formación; Auditorías; Herramientas GRC; Simulacros; Continuidad; Gestión de terceros

FASE 5 — SUPERVISIÓN Y REPORTING

BLOQUE / CATEGORÍA	CONTENIDO	LECTURA EJECUTIVA
5.1 Riesgo	Riesgo residual; Riesgos críticos abiertos; Riesgos fuera de apetito.	Aprobación del modelo de indicadores con foco en exposición, severidad y desviaciones frente al apetito.
5.1 Operación	Vulnerabilidades críticas; Parches críticos; Tiempo de remediación; Coberturas: MFA y EDR.	Seguimiento de capacidad operativa y eficacia de los controles técnicos clave.
5.1 Incidentes	Número de incidentes; Tiempo de detección; Tiempo de contención; Impacto negocio.	Permite evaluar frecuencia, velocidad de respuesta e impacto sobre el negocio.
5.1 Terceros	Terceros críticos evaluados; Incidentes de proveedores.	Visibilidad del riesgo extendido y de la dependencia operativa de proveedores críticos.
5.1 Madurez	Nivel NIS2; Nivel ENS/ISO 27K; Ejecución roadmap.	Mide avance de cumplimiento y evolución de capacidades frente al plan definido.
5.2 Reporte al Consejo	Debe definir: Frecuencia; Formato; Indicadores; Riesgos escalados; Incidentes relevantes; Estado regulatorio; Necesidades presupuestarias.	Recomendación: Comité mensual; Consejo trimestral; Incidentes críticos inmediato.
5.3 Informe ejecutivo CISO	Resumen ejecutivo; Riesgos críticos; Estado del cumplimiento NIS2; Incidentes relevantes; Estado SOC/CSIRT; Vulnerabilidades críticas; Riesgos de terceros; Estado del roadmap; Necesidades de inversión; Decisiones requeridas.	Contenido mínimo para soportar supervisión, priorización y toma de decisiones del Consejo.

FASE 6 — SUPERVISIÓN

6.1 Supervisión de capacidades SOC y CSIRT

La dirección debe verificar periódicamente que las capacidades de detección, análisis, respuesta y escalado son suficientes.

Integradas con negocio, operación y gestión de crisis.

Capacidades operativas

6.2 Gestión de crisis y simulacros ejecutivos

Recomendaciones, por ejemplo, la figura del RSI, el Centro Nacional de Ciberseguridad, los CSIRTs de referencia o las autoridades de control y puntos de contacto sectoriales.

6.3 Supervisión de continuidad de negocio

Aprobación del SoA.

Integración con **Declaración de Aplicabilidad (SoA)**, vinculada al artículo 28 del ENS, para mapear las medidas sobre los activos, un documento que no aparece con ese nivel de detalle en la Directiva.

Aprobación del Plan de continuidad de negocio, como piedra angular de la resiliencia.

FASE 7

SUPERVISIÓN DE TERCEROS

La supervisión de terceros forma parte del modelo de gobierno y control exigido en el paquete de adopción de responsabilidades.

Aprobación del modelo de riesgos de terceros

Debe incluir

- Clasificación de proveedores críticos.
- Due diligence.
- Cláusulas contractuales.
- Derecho de auditoría.
- Requisitos mínimos de seguridad.

Fase 8 — Evidencia Regulatoria y Diligencia Debida

La organización debe mantener un repositorio trazable y actualizado de evidencias que permitan demostrar ante reguladores, auditores y órganos de gobierno que las decisiones, aprobaciones, supervisiones y actividades de capacitación se han realizado de forma efectiva y documentada.

La conservación de evidencias de gobierno, formación y reporting es un elemento central para acreditar cumplimiento bajo NIS2.

Evidencias

Actas del Consejo

Evidencias de formación

Aprobaciones formales

Informes del CISO

Evaluaciones de riesgo

Indicadores

Decisiones de aceptación de riesgo

Simulacros realizados

Auditorías y revisiones

Muchas gracias

¿Preguntas?