

CURSO ESPECIALIZADO: CIBERSEGURIDAD Y RESPONSABILIDAD JURÍDICA EN EL SECTOR PÚBLICO

Directiva NIS2 y nuevo marco legal para el año 2026

¿A QUIÉN VA DIRIGIDO?

- Directivos públicos y gerentes de organismos autónomos
- Responsables jurídicos y de cumplimiento normativo
- Directores de sistemas y responsables de ciberseguridad
- Técnicos de protección de datos y privacidad
- Responsables de seguridad de la información (RSI/CISO públicos)



OBJETIVOS Y VENTAJAS DE ESTA FORMACIÓN

- **Comprender** el nuevo marco normativo derivado de la **Directiva NIS2** y su **trasposición en España**
- **Identificar** las **obligaciones legales** y **responsabilidades patrimoniales** de las AA.PP. ante incidentes de ciberseguridad.
- **Analizar** casos reales para entender sus **consecuencias jurídicas y organizativas**.
- **Proporcionar** criterios prácticos para **prevenir riesgos jurídicos** y **reforzar la seguridad jurídica y operativa**
- **Capacitar** a los responsables jurídicos, técnicos y directivos públicos en la **toma de decisiones estratégicas** sobre ciberseguridad, cumplimiento normativo y gobernanza digital.

IMPARTIDO POR:

D. Víctor Almonacid Lamelas

Consultor jurídico y
estratégico del sector público.
Secretario de la
Administración Local y
Directivo Público Profesional
(excedente)



Madrid, 28 y 29 de abril de 2026

09.30 Inicio y presentación del curso.

MARCO NORMATIVO DE EMERGENCIA: DE LA DIRECTIVA NIS2 AL DERECHO ESPAÑOL

Anteproyecto de Ley de Ciberseguridad: tramitación urgente y entrada en vigor

Obligaciones inmediatas para administraciones públicas como "entidades esenciales"

Diferencias entre entidades esenciales e importantes: régimen jurídico diferenciado

OBLIGACIONES LEGALES ESPECÍFICAS PARA EL SECTOR PÚBLICO.

Evaluación y gestión de riesgos de ciberseguridad: requisitos mínimos

Notificación obligatoria de incidentes: plazos y procedimientos

Esquema Nacional de Seguridad (ENS) como marco de cumplimiento. Relaciones con la Ley Orgánica de Protección de datos.

Auditorías periódicas y certificación obligatoria

11.30 Pausa-café.

12.00 RESPONSABILIDAD PATRIMONIAL POR CIBERATAQUES: ANÁLISIS JURISPRUDENCIAL

Caso SEPE: lecciones aprendidas sobre funcionamiento anormal del servicio

Requisitos de la responsabilidad patrimonial en ciber incidentes

Daño efectivo, evaluable e individualizado en contexto digital

Excepciones: fuerza mayor vs. negligencia administrativa

RÉGIMEN SANCIONADOR Y PODERES DE SUPERVISIÓN

Multas de hasta 10 millones de euros para entidades esenciales

Poderes coercitivos de las autoridades competentes

Responsabilidad personal de directivos: prohibiciones temporales

Suspensión de certificaciones y autorizaciones

14:30 Almuerzo libre.

16:00 GESTIÓN JURÍDICA DEL RIESGO CIBERNÉTICO

Protocolos de actuación ante incidentes: aspecto legal y técnico

Documentación y trazabilidad para defensa jurídica

Seguros de ciber riesgo y cobertura de responsabilidad patrimonial

Cláusulas contractuales con proveedores

17:00 CASOS PRÁCTICOS Y ESTRATEGIAS DE IMPLEMENTACIÓN

Análisis de vulnerabilidades jurídicas en entidades tipo

Elaboración de políticas de seguridad conforme a NIS2

Procedimientos de notificación e interacción con autoridades

Plan de continuidad del servicio público tras ciber incidente

18:00 Clausura

PRESENTACIÓN Y OBJETIVOS DEL CURSO



La ciberseguridad se ha convertido en la prioridad jurídica nº1 del sector público.

En 2026, el nuevo marco legal derivado de la **Directiva NIS2** traerá **obligaciones inmediatas** y **riesgos patrimoniales sin precedentes**.

La trasposición urgente de dicha **Directiva**, obliga a las administraciones a **adaptar su gobernanza digital y jurídica**.

Este curso ofrece una **visión práctica** de las nuevas **obligaciones legales, riesgos patrimoniales y medidas organizativas**.

Una formación esencial para **directivos, técnicos y juristas públicos** ante el nuevo escenario normativo de 2026.

2ª jornada, 29 de abril de 2026

09:00 APERTURA Y RECAPITULACIÓN. Presentación de los objetivos de la jornada.

09:15 BLOQUE I: EL RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN (RSI) EN LAS AA.PP.

Obligatoriedad del RSI. Designación y acreditación por el Ministerio del Interior.

Funciones: elaboración de políticas de ciberseguridad, supervisión, gestión de incidentes y punto de contacto con autoridades.

Responsabilidad personal de los directivos: Art. 14 del Anteproyecto responsabiliza directamente a los órganos de dirección del cumplimiento; posibilidad de prohibición temporal del ejercicio de funciones directivas.

RSI, DPO y el DPA: tres figuras clave en la gobernanza digital de las AA.PP: similitudes y diferencias.

10:15 BLOQUE II: AUDITORÍA ENS Y CERTIFICACIÓN: DE LA TEORÍA A LA PRÁCTICA

El ciclo de auditoría ENS conforme al RD 311/2022: autoevaluación previa, auditoría externa por entidad acreditada (ENAC), informe de conformidad y renovación bienal.

Niveles de seguridad (básico, medio, alto)

Declaración de Conformidad como acreditación ante licitaciones y terceros.

CASO PRÁCTICO: revisión de un Checklist real de preparación para auditoría ENS en una organización pública mediana.

11:00 Pausa-café.

11:20 BLOQUE III: GESTIÓN AVANZADA DE INCIDENTES Y NOTIFICACIÓN LEGAL

Plazos legales de notificación: alerta temprana en 24 h, notificación completa en 72 h, informe final en un mes.

Cadena de notificación: CCN-CERT (sector público), Centro Nacional de Ciberseguridad como punto de contacto único. Coordinación entre administraciones, divulgación coordinada de vulnerabilidades. Obligación de las entidades afectadas de cooperar en la identificación y tratamiento.

Caso real: análisis de la gestión del incidente del SEPE y su comparación con los nuevos protocolos NIS2 (*continuación del caso introducido en la Primera Parte*)

12:10 BLOQUE IV: CIBERSEGURIDAD EN LA CONTRATACIÓN PÚBLICA Y CADENA DE SUMINISTRO

Obligaciones NIS2 respecto a proveedores TIC y cadena de suministro: evaluación de riesgos de terceros.

Cláusulas contractuales obligatorias en contratos de servicios digitales con la Administración: SLA de seguridad, auditorías y derecho de inspección. El Reglamento DORA: afectación para el sector público.

Pliegos de prescripciones técnicas de seguridad: cómo exigir certificación ENS a los proveedores.

Taller práctico: redacción de una cláusula de ciberseguridad para un contrato de servicios en la nube con una entidad local.

12:55 BLOQUE V: RESILIENCIA, CONTINUIDAD Y ESTRATEGIA PARA 2026 Y MÁS ALLÁ

Plan de Continuidad del Servicio Público (PCSP): diferencias con el plan de recuperación ante desastres (DRP); obligatoriedad ENS nivel medio-alto. Pruebas de resiliencia: simulacros de ciber incidente y evaluación de resultados.

El Centro Nacional de Ciberseguridad: nuevo actor institucional.

Inteligencia artificial y ciberseguridad: riesgos emergentes en el sector público y primeras respuestas normativas (Reglamento IA UE).

13:40 CLAUSURA Y SESIÓN DE PREGUNTAS.

Resolución de dudas y casos planteados durante la jornada.

14.00 Fin de la jornada

FECHA Y LUGAR DE CELEBRACIÓN

 Madrid – 28 y 29 de abril de 2026
 Hotel Gran Versalles – C/ Covarrubias 4-6

FORMAS DE INSCRIPCIÓN Y CONTACTO

Telefónica: 669 521 789
e-mail: inscri@renher.es

 **A través de este enlace**

Para formalizar su inscripción, necesitamos que nos envíen los siguientes datos:

Nombre y apellidos del asistente
Departamento en el que trabaja
Empresa o entidad
CIF de la entidad
Dirección, código postal y población
Teléfono de contacto

E-mail DE LA PERSONA QUE VAYA A ASISTIR
(IMPRESINDIBLE)

Forma de facturación PREFERIDA: electrónica o convencional, mediante factura emitida en PDF con firma, y a dónde y/o a quién debe ser enviada la factura.

PRECIO, DESCUENTOS Y TARIFAS ESPECIALES

 Precio **797 € más 21 % de IVA**

En caso de que de su institución o empresa deseen inscribir a varias personas, **LA 4ª INSCRIPCIÓN SERÁ GRATUITA.**
Si Ud. ya ha venido a alguno de nuestros cursos, tendrá un **10% de DESCUENTO** por ser antiguo cliente.

FORMAS DE PAGO

Transferencia Bancaria CAIXABANK
Titular: ODRICERIN & ASOCIADOS
Nº C.C. ES80 2100 3737 0222 0037 4365

CERTIFICADO DE ASISTENCIA

Todos los alumnos recibirán por correo electrónico un certificado acreditativo de su asistencia a este curso.

FORMACIÓN INTERNA

Todos nuestros cursos se ofrecen también como formación interna, con las adaptaciones necesarias a las necesidades de cada cliente.

CANCELACIONES

Toda cancelación recibida una semana antes de la celebración del curso, tendrá derecho a la devolución de los derechos de inscripción descontando un 10 % en concepto de gastos.

Las bajas posteriores a este plazo recibirán un bono de asistencia para cualquier otra conferencia, con los necesarios ajustes de precio en su caso. En cualquier momento, una persona inscrita puede ser sustituida por otra de la misma empresa.¹

BONIFICACIONES

Esta formación puede ser bonificada a través de los créditos de la Fundación Estatal para la Formación en el Empleo. Contamos con un servicio de bonificación de esta formación.

Si tiene interés en ella, pónganse en contacto con Mar González 915102326 m.gonzalez@consultae.es



ODRICERIN
Cursos de Formación