Obligaciones de notificación de incidentes de ciberseguridad en España

La actividad profesional en ciberseguridad en España implica el conocimiento y cumplimiento de obligaciones legales de notificación de incidentes. No se trata únicamente de conocimiento teórico, sino de exigencias aplicables en la práctica diaria. Existe un ecosistema de notificación compuesto por múltiples actores y normas. La obligación de notificar depende principalmente de:

Quién es la entidad afectada (naturaleza jurídica y sector).

Qué ha ocurrido (tipo e impacto del incidente).

El sistema normativo puede estructurarse en tres grandes capas regulatorias, cada una con su ámbito de aplicación y autoridades competentes.

1. La Capa Clásica: El Esquema Nacional de Seguridad (ENS) para el Sector Público

Las administraciones públicas tienen sus reglas.

- **Ámbito:** Sector Público (Administración General del Estado, Comunidades Autónomas, Entidades Locales como ayuntamientos, universidades públicas, etc.). Empresas que los proveen.
- **Obligación:** Deben notificar los incidentes con un impacto **ALTO, MUY ALTO o CRÍTICO** en la seguridad de los sistemas de información, según su categorización en el ENS .
- **¿A quién?** Al **CCN-CERT** (Centro Criptológico Nacional-CERT), que es su CSIRT de referencia.
- **¿Cómo?** ¿Cómo? Preferentemente a través de la herramienta LUCÍA, accesible mediante navegador. Dependiendo del organismo, se utilizará el servidor central del CCN o una instancia propia federada en su propio CPD. La comunicación sigue la taxonomía estandarizada de la Guía CCN-STIC 817, asegurando que toda la Administración hable "el mismo idioma".

  Preferentemente a través de la herramienta **LUCÍA**, La notificación debe realizarse de forma automatizada o a través de la plataforma, quedando el correo electrónico como vía subsidiaria. Lucia se accede a través del navegador, donde se completa un formulario del incidente. Se puede acceder al servidor central de la CCN o un servidor instalado en el propio CPD de la institución.

Las definiciones y criterios se encuentran principalmente en:

- El **Real Decreto 311/2022**, por el que se regula el ENS (norma actualmente vigente).
- La directiva **NIS2**, que está en proceso de implantarse.
- Sus **Instrucciones Técnicas de Seguridad (ITS)**.
- Las **guías CCN-STIC** elaboradas por el Centro Criptológico Nacional.

2. La Capa de "Protección de Datos": El RGPD para Violaciones de Datos Personales

Esta obligación es transversal y aplica a **cualquier organización** (pública o privada) que trate datos personales.

- **Ámbito:** Cualquier responsable del tratamiento de datos (empresas, autónomos, asociaciones, administraciones públicas...).
- **Obligación:** Notificar cualquier **violación de la seguridad de los datos personales** (ej. pérdida, robo, acceso no autorizado a datos de clientes, empleados, etc.). Es importante que no es necesario que una institución pública o privada notifique cualquier incidencia al AEPD, sólo las brechas de datos personales. Solo se notifica a la AEPD si hay una "violación de la seguridad de los datos personales" (confidencialidad, integridad o disponibilidad de datos de personas físicas).
- **¿A quién?** A la **Agencia Española de Protección de Datos (AEPD)**. **El formulario de la AEPD:** Al igual que con LUCÍA, la AEPD tiene su propia **Sede Electrónica**. No se manda un correo; se rellena un formulario web estructurado donde se pide: Naturaleza de la brecha. Categorías de datos afectados (DNI, salud, correos...). Número aproximado de interesados. Medidas tomadas para paliar el daño.
- Doble notificación. Si un Ayuntamiento sufre un Ransomware que cifra los expedientes de los ciudadanos. Notifica al **CCN-CERT** por ser un incidente de impacto alto en la Administración (vía LUCÍA). Notifica a la **AEPD** porque ha habido una pérdida de disponibilidad y confidencialidad de datos personales (vía Sede Electrónica AEPD).
- **Plazo crítico:** A más tardar **72 horas** después de que se tenga constancia de la brecha . Si el riesgo es "alto", además, se debe comunicar a los propios afectados .

La AEPD tiene una herramienta llamada **"Comunica-Brecha"** que es un motor de decisión (un cuestionario breve) que ayuda a decidir si debes notificar o no.

3. La Capa de "Servicios Esenciales": La Directiva NIS y su evolución a NIS2

Esta es, probablemente, el área de mayor complejidad y actualidad, y donde no solo interviene el CCN, sino también INCIBE y otras autoridades. La normativa de referencia ha sido el *Real Decreto-ley 12/2018*, pero está en pleno proceso de actualización por la nueva **Directiva NIS2**.

NIS2 en España: situación normativa actual

1. Marco europeo

La norma europea actualmente vigente es la Directiva (UE) 2022/2555 (NIS2). Sustituye a la anterior Directiva NIS (2016). Introduce: Nuevas categorías: entidades esenciales e importantes. Plazos estrictos de notificación (24h, 72h, informe final en 1 mes). Régimen sancionador más severo. Como directiva, no es directamente aplicable: necesita transposición al derecho interno.

2. Situación en España

La norma actualmente en vigor que transpone la primera NIS es el Real Decreto-ley 12/2018, desarrollado por el RD 43/2021. Este régimen sigue siendo el marco jurídico plenamente aplicable mientras no entre en vigor la ley española de transposición de NIS2.

España ha estado en proceso de adaptación normativa a NIS2.

3. NIS2: Lo que hay que saber en 2026

La Directiva **NIS2** expande drásticamente el número de entidades obligadas a protegerse y notificar incidentes. En España, el nuevo marco legal (que evoluciona el RD-ley 12/2018) establece que:

•**Nuevas Categorías:** Ya no hablamos solo de "operadores de servicios esenciales", sino de **Entidades Esenciales** (energía, salud, banca) y **Entidades Importantes** (gestión de residuos, alimentación, servicios postales).

•**Notificación en tres pasos:** Se acaba la flexibilidad. Hay que enviar una **alerta temprana (24h)** para avisar de que algo pasa, una **notificación oficial (72h)** con detalles del impacto, y un **informe final (1 mes)** con las lecciones aprendidas.

•**Responsabilidad de la Dirección:** Los órganos de administración (directores, alcaldes) son responsables directos si no se cumplen las medidas de seguridad, pudiendo ser sancionados personalmente.

•**Cadena de Suministro:** Las entidades deben vigilar no solo su seguridad, sino la de sus proveedores tecnológicos.

4. El papel de INCIBE en la notificación

El **INCIBE-CERT** es el centro de respuesta de referencia para el **sector privado y la ciudadanía**. Su papel es fundamental por tres motivos:

1.Notificación Obligatoria (NIS2 Privada): Las empresas privadas que sean "Entidades Esenciales o Importantes" bajo NIS2 y no sean críticas para la Defensa, deben notificar sus incidentes al **INCIBE-CERT**. Es el "equivalente" al CCN-CERT pero para el mundo empresarial.

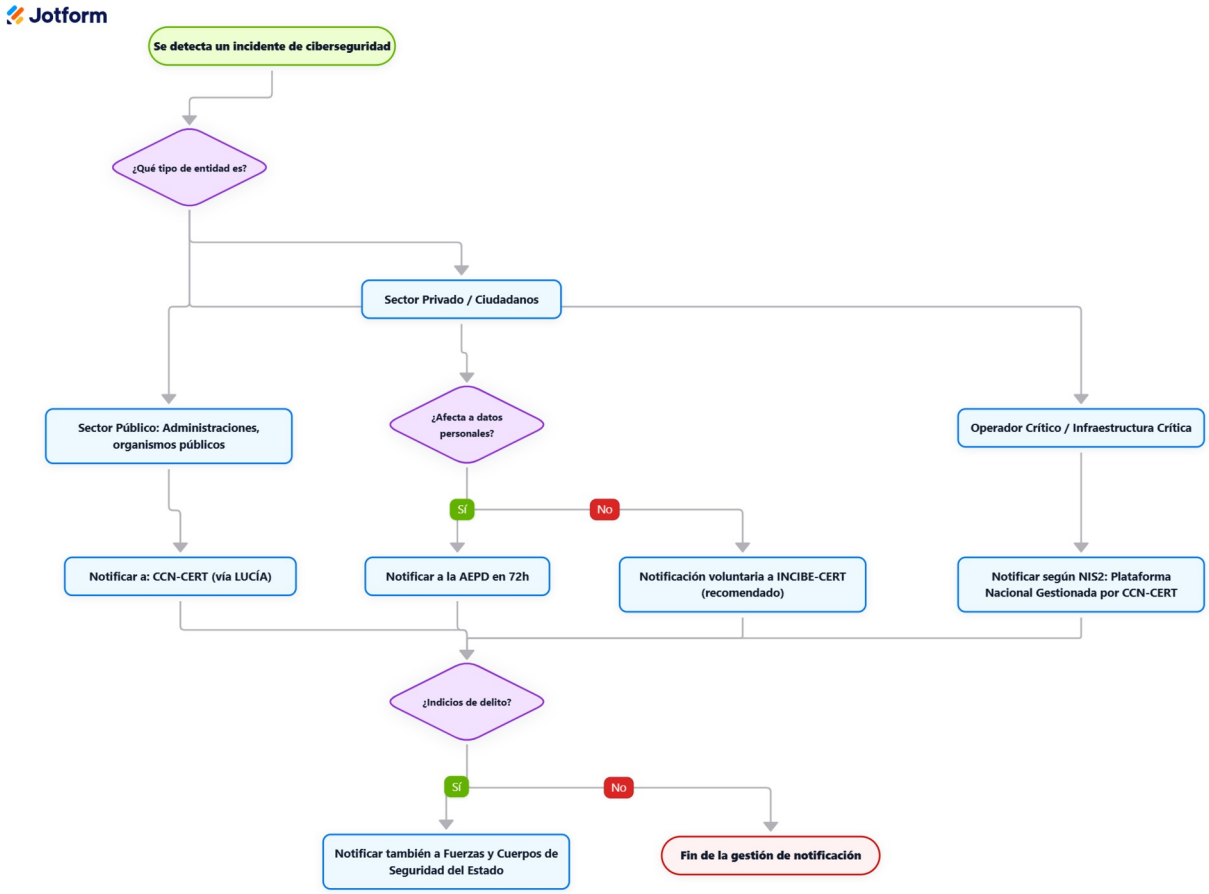
2.Notificación Opcional (Cualquier empresa/ciudadano): Cualquier PYME o ciudadano que sufra un incidente (fraude, ransomware, phishing) puede reportarlo al INCIBE de forma voluntaria para recibir soporte técnico y ayudar a prevenir ataques similares en el resto de España.

3.Colaboración con el CCN: INCIBE y CCN operan de forma coordinada. Si una empresa privada que da servicio a un Ayuntamiento es atacada, ambos centros comparten información para proteger tanto el servicio público como el tejido empresarial.

4. Otras Instituciones y Circunstancias

La notificación no siempre termina en el CCN, INCIBE o la AEPD. Dependiendo de la naturaleza del incidente, pueden aparecer otros organismos:

- **El CSIRT de referencia para ciudadanos y empresas "comunes":** El **INCIBE-CERT** (Instituto Nacional de Ciberseguridad) es el punto de contacto para ciudadanos y empresas del sector privado que **no** están obligadas por normativas sectoriales (NIS, ENS...). Para estas, la notificación es voluntaria, pero altamente recomendada .
- **Infraestructuras Críticas:** Si el incidente afecta a un operador crítico (sectores estratégicos como energía, transporte, agua...), entra en juego el **CNPIC** (Centro Nacional de Protección de Infraestructuras y Ciberseguridad) .
- **Ámbito Militar y Defensa:** El **ESP-DEF-CERT** es el responsable de las redes y sistemas de las Fuerzas Armadas y la Defensa Nacional .
- **Fuerzas y Cuerpos de Seguridad del Estado (FCCSE):** Si el incidente tiene indicios de delito (ej. un ataque de ransomware con extorsión), además de las notificaciones obligatorias por normativa, se debe poner en conocimiento de las FCCSE (Policía Nacional, Guardia Civil) para que inicien la investigación .
- **Supervisores Financieros:** Como bien apunta un artículo sobre NIS2, si el incidente afecta a una entidad financiera (banco, aseguradora), puede haber obligación de notificar también al **Banco de España** o a la **CNMV** (Comisión Nacional del Mercado de Valores), especialmente en el marco del reglamento europeo **DORA** (Digital Operational Resilience Act) .



Qué es el ENS

ENS: El Esquema Nacional de Seguridad (ENS) es la normativa española que establece la política de seguridad para proteger los sistemas de información del sector público. Determina principios básicos, requisitos mínimos y medidas de seguridad proporcionales al riesgo, garantizando la confianza en los servicios, la protección de datos y la continuidad de las operaciones de las administraciones públicas.

Real Decreto 3/2010

Real Decreto 311/2022

CERT

CSIRT