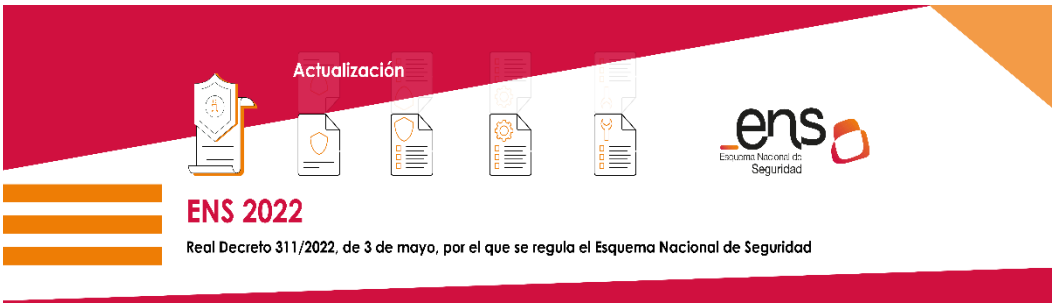
EL NUEVO ESQUEMA NACIONAL DE SEGURIDAD: APLICACIÓN A LAS EMPRESAS DEL SECTOR PRIVADO

Vicente Moret
Of Counsel
vicente.moret@es.andersen.com
Cristina Durante
Associate
cristina.durante@es.andersen.com



El pasado día 3 de marzo, se publicó ***el Real Decreto 311/2022*** *por el que se regula el Esquema Nacional de Seguridad (ENS). Esta norma deroga el anterior ENS de 2010*

- ***El nuevo ENS se aplicará a los sistemas de información de las entidades del sector privado, cuando en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público.***

- ***Procedimientos de licitación de contratos públicos: en los pliegos, se deberán contemplar todos los requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.***

El cambio del marco regulador es sustancial y se recomienda a todas las empresas incluidas en el ámbito de aplicación, que evalúen de inmediato el impacto de esta norma en su negocio, así como su nivel de alineamiento con el nuevo ENS.

ANTECEDENTES

- El ENS es sin duda una **norma jurídica** de la máxima relevancia que regula la seguridad digital a nivel nacional.
- EL ENS es la referencia normativa central a la hora de configurar los **sistemas de gobernanza** de la seguridad digital en las organizaciones. Consiste en un conjunto normativo que posibilita crear y mantener las condiciones necesarias de seguridad en el uso de los medios electrónicos, a través de medidas que garanticen la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos.
- Hasta ahora el ENS se regulaba en el RD 3/2010, y **sólo era aplicable** de forma preferente a las Administraciones Públicas.

LA NUEVA APLICABILIDAD DEL ENS A LAS EMPRESAS DEL SECTOR PRIVADO

- La novedad más relevante del nuevo ENS es precisamente la extensión de su ámbito de aplicación, que sale del estricto alcance anterior limitado al sector público. A partir de ahora una gran cantidad de **empresas privadas se verán obligadas a cumplir con las regulaciones incluidas en el ENS.**
- Así se extrae del artículo 2.3 que establece la **directa aplicación del ENS empresas del sector privado**:
  - → Cuando exista una **relación contractual** y **presten servicios** o provean soluciones a las entidades del sector público.
  - → Cuando los **pliegos** de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector contemplen la necesidad de cumplir requisitos necesarios para asegurar la **conformidad con el ENS** de los sistemas de información en los que se sustenten los servicios prestados por los contratistas.
  - → Cuando se exija en los procedimientos de contratación pública la presentación de las correspondientes **Declaraciones o Certificaciones de Conformidad con el ENS**.
- Además, la aplicabilidad del ENS se extiende también a la ***Supply Chain*** de esas empresas privadas contratistas en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos, según establece el nuevo marco regulatorio.

ASPECTOS MÁS DESTACADOS PARA LAS EMPRESAS DEL SECTOR PRIVADO DEL NUEVO ENS

- Será exigible a estas empresas privadas la aprobación de una **Política de Seguridad por el órgano que ostente las máximas competencias ejecutivas**, con el contenido mínimo y requisitos que marca el artículo 12 del nuevo ENS.
- Ello supone por tanto dotar de **certeza jurídica al contenido, estructura y obligaciones** de las Políticas de Seguridad que deben aprobar las empresas
- Se introducen y regulan normativamente unos **principios básicos** que se pueden aplicar de forma universal como base para construir un **sistema sólido de gobernanza de la seguridad digital**.
  - → Seguridad como proceso integral.
  - → Gestión de la seguridad basada en los riesgos.
  - → Prevención, detección, respuesta y conservación.
  - → Existencia de líneas de defensa.
  - → Vigilancia continua.
  - → Reevaluación periódica.
  - → Diferenciación de responsabilidades.
- Desde el punto de vista de la organización de las empresas, este último principio de **diferenciación de responsabilidades** es muy relevante, ya que por primera vez se ordenan de modo taxativo las diferentes funciones de los responsables: responsable de la información; responsable del servicio; el responsable de la seguridad y el responsable del sistema.
- Además, la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la **explotación de los sistemas** de información.
- Además, se asienta el principio de que la seguridad de los sistemas de información deberá comprometer a **todos los miembros de la organización** y por ello deberá ser conocida por todas las personas que formen parte de la organización.
- En el caso de servicios de seguridad digital externalizados, la organización prestataria de dichos servicios deberá designar un **POC** (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado.

Para más información: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

Madrid; 4 de mayo de 2022