II
ENCUENTRO
DEL ENS

DIEZ AÑOS DE NUEVOS
RETOS Y SOLUCIONES

La relevancia del marco regulador de las certificaciones de ciberseguridad en la nueva ENS

Vicente Moret Millás
***Of Counsel* Andersen Tax & Legal**
Letrado de las Cortes Generales

centro criptológico nacional

En colaboración con:

FEMP
FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

Índice

1. Las certificaciones de seguridad y el ENS
2. El CCN y su función como certificador
3. El nuevo marco europeo de certificación
4. Las oportunidades del nuevo contexto
5. Los próximos avances

1. Las certificaciones y el ENS

- Las certificaciones de seguridad son elementos cada vez más importantes para conseguir un adecuado nivel de seguridad en cualquier organización pública o privada.

- La evaluación y certificación de un producto de seguridad TIC es el **único medio objetivo** que permite valorar y acreditar la capacidad de un producto para manejar información de forma segura.

Cybersecurity matters more than ever during the coronavirus pandemic

WORLD ECONOMIC FORUM

- En el ámbito del **ENS**, el art 18 del RD 3/2010 que lo regula ya entendió su relevancia

  - Adquisición de productos de seguridad y contratación de servicios de seguridad. *Aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición*,
  - La certificación; *según las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.*
  - Organismo de Certificación, determinará el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación,

La relevancia legal de la certificación en el marco de ENS

- La máxima posible, al incluirse en la Ley 40/2015, de Régimen Jurídico del Sector Público. Artículo 156. Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.

2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

2. El CCN y su rol como certificador

- Autoridad Administrativa: Real Decreto 421/2004 de regulación del CCN.
  - *Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y autoridad de certificación criptológica*.
  - *Organismo de certificación del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, de aplicación a productos y sistemas en su ámbito.*

- Orden PRE/2740/2007 Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

  - Certificación. Determinación, obtenida mediante un proceso metodológico de evaluación, de la conformidad de un producto con unos criterios preestablecidos: Funcional, Criptológica, Tempest.

  - Ámbito de actuación del Organismo de Certificación comprende las entidades públicas o privadas que ejerzan de laboratorios acreditados de evaluación de la seguridad de las TI en el marco del ENS.

  - Certificación funcional. *Culminación de un proceso **de evaluación** de las funciones de seguridad de un producto o sistema (objeto de evaluación) que, siguiendo una **metodología también estándar**, realiza un **laboratorio independiente**, acreditado y capacitado técnicamente para tal fin. Se trata de comprobar que el objeto de evaluación realiza correcta y eficazmente la funcionalidad de seguridad que se describe en su documentación. Supone el reconocimiento de la **veracidad** de las propiedades de seguridad de su correspondiente Declaración de Seguridad.*

- El resultado es la inclusión en el Catálogo de Productos STIC (CPSTIC) que ofrece un listado de productos de Seguridad TIC, con unas garantías de seguridad contrastadas, a organismos del Sector Público o entidades privadas que den servicio a éstos y que se encuentren afectados por el Esquema Nacional de Seguridad (ENS) o manejen información clasificada.

- **Base normativa Certificación funcional de la seguridad de las TI**,

✓ Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información,
✓ Normativa interna adaptada UNE-EN ISO/IEC 17065, para reconocimiento nacional.
✓ «Arreglo de Reconocimiento de Certificados de Criterios Comunes» (CCRA), para reconocimiento internacional.

3. El nuevo marco europeo de certificación

- El nuevo contexto de transformación digital acelerada por el COVID acelerada está siendo precipitado, desorganizado e inseguro.

  - Resultado: Aumento importante de la superficie de ataque en todas las actividades económicas y en la sociedad en general.

- Existe una nueva percepción del riesgo en las sociedades occidentales. Se produce un **CAMBIO DE PARADIGMA** que supone la búsqueda de seguridad y certezas.

- Los Estados van a incrementar su **INTERVENCIÓN REGULATORIA** en materias que se consideran esenciales, en sectores considerados críticos o estratégicos para la Seguridad Nacional.

- Los distintos aspectos relativos a la ciberseguridad se van a convertir en centrales, tanto para la Unión Europea como para los Estados, incrementando la actividad regulatoria, de control, sancionadora y de fomento en esa área.

- En el contexto de transformación digital actual esa regulación se va a acelerar porque las agendas políticas de los Gobiernos van a priorizar la resiliencia de la sociedades.

Ya está en vigor un marco jurídico en materia de ciberseguridad que impone obligaciones de cumplimiento normativo.

Nivel Europeo

- Reglamento UE 2019/881 relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación.
- Directiva 2019/713, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo.
- Directiva UE 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información. NIS
- Reglamento UE 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Reglamento UE 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Nivel Nacional

- Guía Nacional de Notificación y gestión de ciberincidentes. Consejo Nacional de Ciberseguridad, 9 de enero de 2019.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Proyecto de Reglamento de desarrollo Real Decreto-Ley 12/2018 de seguridad de las redes y sistemas
- Real Decreto-Ley 12/2018 de información. (Trasposición Directiva NIS).
- Real Decreto-ley 19/2018 de servicios de pago y otras medidas urgentes en materia financiera.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las Infraestructuras Críticas.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS).

- El contexto actual de búsqueda de certezas en un mundo totalmente dependiente de lo digital, coloca a las certificación de ciberseguridad de productos, sistemas y servicios todavía más en el centro de atención.

- Pero el panorama actual global de las certificaciones está fragmentado y disperso. ***Common criteria*** es el estándar más utilizado: Fiable, robusto, reconocido internacionalmente, pero complejo y coste elevado.

- **Tendencias hoy**

  - Utilizar *Common Criteria* como base de procesos de certificación privados.

  - Esquemas de certificación propios impulsados por Gobiernos.

  - Nuevas certificaciones ligeras; más fáciles de obtener, para niveles de seguridad sustancial y básico pero no alto. LINCE. Vulnerabilidades y Pentest.

- En este contexto la UE ,después del esfuerzo de poner en marcha NIS, con el vector RGPD ya en funcionamiento, decide dar un paso más y aprueba el **Reglamento 2019/881** relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información.

The EU Cybersecurity Act has made a dramatic change in the domain of cybersecurity evaluation by creating a single framework federating different evaluation schemes to harmonize Cybersecurity evaluation across the EU and therefore ***create a single European Cybersecurity Market.*** *A unified certification framework across all of EU reduces the effects a fragmented market has on the economy.*

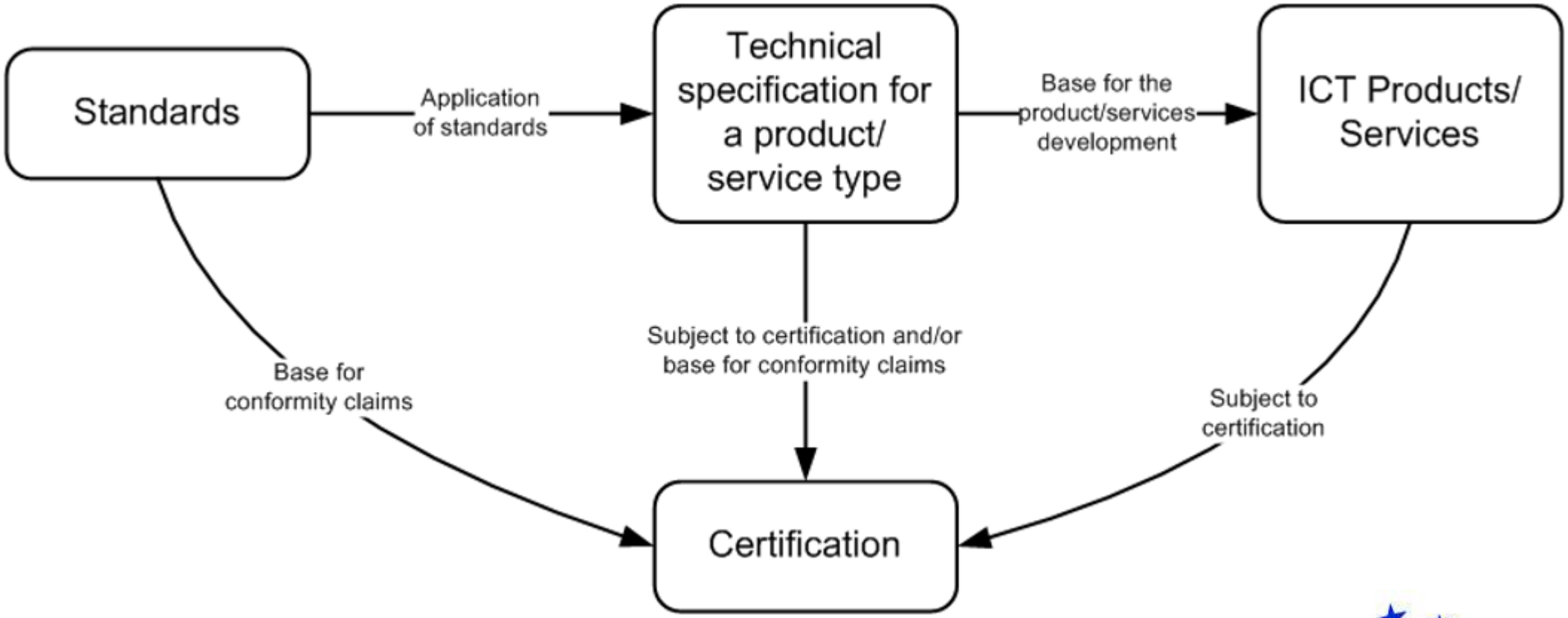
❑ **Establece 4 fases**:

1.- Creación del Union Rolling Working Programme (URWP)
2.- Preparación de un esquema común aceptado.
3.- Aprobación mediante normativa europea del esquema.
4.- Implementación del nuevo esquema por parte de los Estados miembros.

- ❑ En estos momentos se está llevando a cabo el proceso de negociación en el cual los Estados están intentando que el nuevo esquema recoja en lo máximo posible las características de los esquemas nacionales ya implantados y en funcionamiento desde hace años.

- ❑ Se puede anticipar que dependiendo del nivel de ciberseguridad requerido, el nivel de certificación variará:

  - ❑ Desde la declaracion responsable por el propio proveedor o fabricante,
  - ❑ Hasta la intervención de la autoridad nacional de certificación.


Standards
Application of standards
Technical specification for a product/ service type
Base for the product/services development
ICT Products/ Services
Base for conformity claims
Subject to certification and/or base for conformity claims
Subject to certification
Certification

- A este respecto hay que mencionar que **según ENISA**, España se situa entre los países a tener en cuenta en esta configuración, ya que es de los pocos que tienen certificaciones ya en funcionamiento que deben acompañar a los standares que se seleccionen: *lightweight certification schemes such as the CSPN (France), the BSZ (Germany), LINCE (Spain) and BSPA (Netherlands).*

- Otro elemento importante es que ENISA quiere extender los esquemas de certificación europeos además de a productos, servicios y procesos finales, también a los procesos de ingeniería fijando líneas maestras para el desarrollo del software.

4. Las oportunidades del nuevo contexto

- Nunca antes el contexto fue tan propicio a la potenciación de las certificaciones como mecanismo de aumentar la ciberseguridad total de Administraciones, Empresas y de la sociedad en general.

- La nueva regulación va a aumentar la demanda de productos certificados y no solo en Administraciones Públicas. Las empresas también demandarán estos productos certificados. Especialmente las que sean calificadas como Operadores de Servicios Esenciales y Prestadores de Servicios Digitales.

- Estas tendencias se recogen en las ultimas comunicaciones de la Comisión Europea: *Shaping Europe´s Digital Future* y el *Recovery Plan.*

- Muy probablemente la certificación se convierta en requisito para los procesos de contratación pública a todos los niveles.

- No obstante, otro factor a tener muy en cuenta es el de la **virtualidad jurídica** de las certificaciones de ciberseguridad en relación con el creciente número de normas que forman parte del *compliance* específico de ciberseguridad que deben cumplir las empresas privadas de todo tipo.

- En este sentido las certificaciones de los productos y servicios son una herramienta jurídica de primer orden para demostrar la **diligencia debida** con respecto a las responsabilidades ante un ciberincidente:

  - Administrativas; por los procedimientos sancionadores del RD ley 12/2018 o del RGPD.
  - Civiles, por los daños ocasionados a terceros.
  - Incluso penales en su caso.

  La utilización de productos y sistemas certificados contribuirían en gran medida a mitigar o eludir incluso esas posibles responsabilidades

- La exigencia de una política de exigencia de certificaciones respecto a terceros debe formar parte del mapa de riesgos legales y de políticas propias de toda organización en el marco del cumplimiento normativo en materia de ciberseguridad.

- El **nuevo Reglamento de desarrollo del RD Ley 12/2018, NIS**, a punto de ser aprobado, recoge la necesidad de adoptar por parte de OSE y PSD de *Medidas para el cumplimiento de las obligaciones de seguridad,* entre las cuales se cuenta la de disponer de una política de adquisición de productos o servicios de seguridad*.*

- Se incluirá en la *Declaración de Aplicabilidad de medidas de seguridad,* que será suscrito por el Responsable de Seguridad del sistema de información del operador y comunicada a la Autoridad como compromiso.

- Además se reconduce al ENS que será el marco de referencia para esos OSE y PSD

Las medidas a las que se refieren los apartados anteriores tomarán como referencia las recogidas en el anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en la medida en que sean aplicables, y se basarán, cuando sea posible, en otros esquemas nacionales de seguridad existentes.

5. Los próximos avances

- La revisión de la Directiva NIS está en marcha en Bruselas y con seguridad las certificaciones jugarán un papel importante.
- Las infraestructuras críticas, especialmente las digitales, verán incrementada la la carga normativa de cumplimiento en cuanto a productos y servicios certificados.
- Los primeros estándares específicos que desarrollará la UE irán destinados a dispositivos conectados en redes 5G y a servicios cloud.
- El proceso por parte de ENISA se va a acelerar previsiblemente tras la situación de inseguridad generada por la Pandemia.

Qué debería hacer España…

- ✓ La revisión de ENS es el mejor contexto posible para elevar el sistema de certificación al lugar que debe ocupar como elemento que permite dotar de **certezas** a la situación actual de ciber-inseguridad en un contexto VUCA.

- ✓ Promover que no sólo las Administraciones sino también las empresas privadas se certifiquen en el ENS, lo cual aumenta la resiliencia total del país y su implicación en el esfuerzo colectivo que supone

- ✓ Dotar de **fuerza jurídica a las obligaciones de certificación** tanto para Gobierno y Administraciones como para OSE y PSD en la revisión que se deba producir tanto del ENS como del ámbito NIS.

- ✓ La obligatoriedad en la utilización de certificaciones reconocidas debe ser reforzada mediante un nuevo tipo de sanción grave en la revisión de NIS para ciertos sistemas y empresas.

- ✓ Reforzar las obligaciones al respecto en materia de contratación pública.

- ✓ Defender en el momento actual la bien asentada estructura de certificación española para que en el nuevo marco europeo de certificación que está naciendo, **los procesos de certificación que lleva a cabo el CCN tengan reconocimiento y homologación al máximo nivel posibles.** Las certificaciones nacionales deben insertarse directamente en el nuevo esquema europeo sin necesidad de procedimientos de reevaluación.

- ✓ Favorecer al ecosistema de laboratorios que ya existen en España como posible vector de generación de negocio a escala europea e internacional de forma tal que se conviertan en referente mundial a la hora de obtener certificaciones que abrirán el mercado europeo a esos productos y servicios.

- ✓ Favorecer y sacar el máximo partido a las certificaciones ligeras como LINCE que permiten realizar un análisis rápido y eficaz de cara a insertar los productos en el mercado con prontitud.

- ✓ Promover que en las distintas normativas que regulen los sectores considerados estratégicos en el RD Ley 12/2018 (financiero, agua, transportes, telecomunicaciones, energía…) incluyan de forma expresa referencias a la obligatoriedad de utilizar productos certificados y que además incluyan expresamente que su uso será indicio cualificado de un adecuada diligencia debida de cumplimiento normativo.

- ✓ Generar conciencia y cultura de ciberseguridad en la sociedad en general y en concreto acerca de la necesidad de usar productos y servicios certificados.

II ENCUENTRO DEL ENS

DIEZ AÑOS DE NUEVOS RETOS Y SOLUCIONES

centro criptológico nacional

En colaboración con:

FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

GOBIERNO DE ESPAÑA · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

Muchas gracias.

Estratégicos

Estándar