jtsec
BEYOND IT SECURITY

Estándares y certificaciones

en materia de productos ciberseguros en Europa

Javier Tallón Guerri

jtsec Beyond IT Security

jtallon@jtsec.es

@javiertallon

- Ingeniero en Informática (Universidad de Granada)
- Co-Fundador & Director Técnico en itsec Beyond IT Security S.L.
- Experto en Common Criteria, LINCE, …
- Miembros del grupo de trabajo Ad-hoc SOG-IS en la Agencia Europea de Ciberseguridad ENISA y del SCCG (Stakeholders Cybersecurity Certification Group)
- Colaboramos en diversos foros de estandarización como ISO o CEN/CENELEC
- OSCP/OSCE/CISSP

CONTENIDO

CONTENIDO

El apasionante mundo de la auditoria de ciberseguridad

El apasionante mundo de la auditoria de ciberseguridad

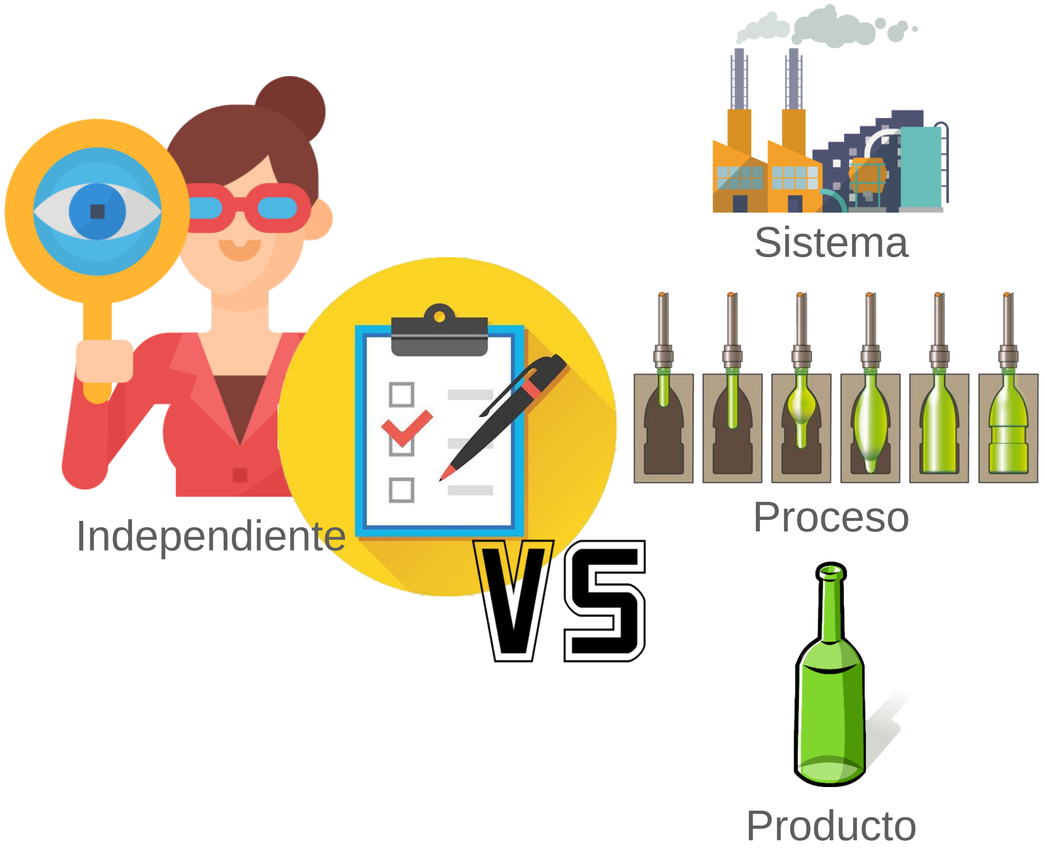
El apasionante mundo de la auditoria de ciberseguridad

El apasionante mundo de la auditoria de ciberseguridad

El apasionante mundo de la auditoria de ciberseguridad

- **Auditoría:** *Mecanismo de control **independiente** del sistema controlado, que siguiendo una **metodología** compara una serie de características con respecto a **pautas, normas o estándares** con el objetivo de encontrar desviaciones.*

- Pueden ser internas o realizadas por un tercero



El apasionante mundo de la auditoria de ciberseguridad

Algunos tipos de auditorías comunes en Ciberseguridad

- Auditoría técnica de un sistema o un producto
  - Por profundidad
    - Análisis de vulnerabilidades automatizado
    - Pruebas de penetración
    - Red Team / Blue Team / Purple Team
- Por conocimiento
    - Caja blanca / Caja negra / Caja gris
- Por alcance
    - Perimetral / interna / wifi / …
- Por ser demasiado tarde:
  - Análisis forense

El apasionante mundo de la auditoria de ciberseguridad

Algunos tipos de auditorías comunes en Ciberseguridad

- Auditoría no técnica
  - Análisis de riesgos
  - Seguimiento de buenas prácticas
  - Cumplimiento de una norma
  - Compliance
    - Notificación de incidentes
  - Seguridad gestionada (SGSI)
    - Indicadores
    - Políticas

El apasionante mundo de la auditoria de ciberseguridad

¿Por qué auditar?

- Independencia crítica
- Es mejor auditarte tu mismo antes de que un ciberdelincuente te audite.

El apasionante mundo de la auditoria de ciberseguridad

¿Qué clase de pruebas puedo esperar en mi sistema?

Técnicas

- Ataques a las redes wifi
- Rogue Aps
- Ataques al directorio activo
- Ataques de fuerza bruta / diccionario
- Uso de keyloggers
- USB Dropping
- Ataques de phishing/vishing/ingeniería social
- Búsqueda de vulnerabilidades públicas
  - Explotación de las mismas

El apasionante mundo de la auditoria de ciberseguridad

¿Qué clase de pruebas puedo esperar en mi sistema?

No técnicas

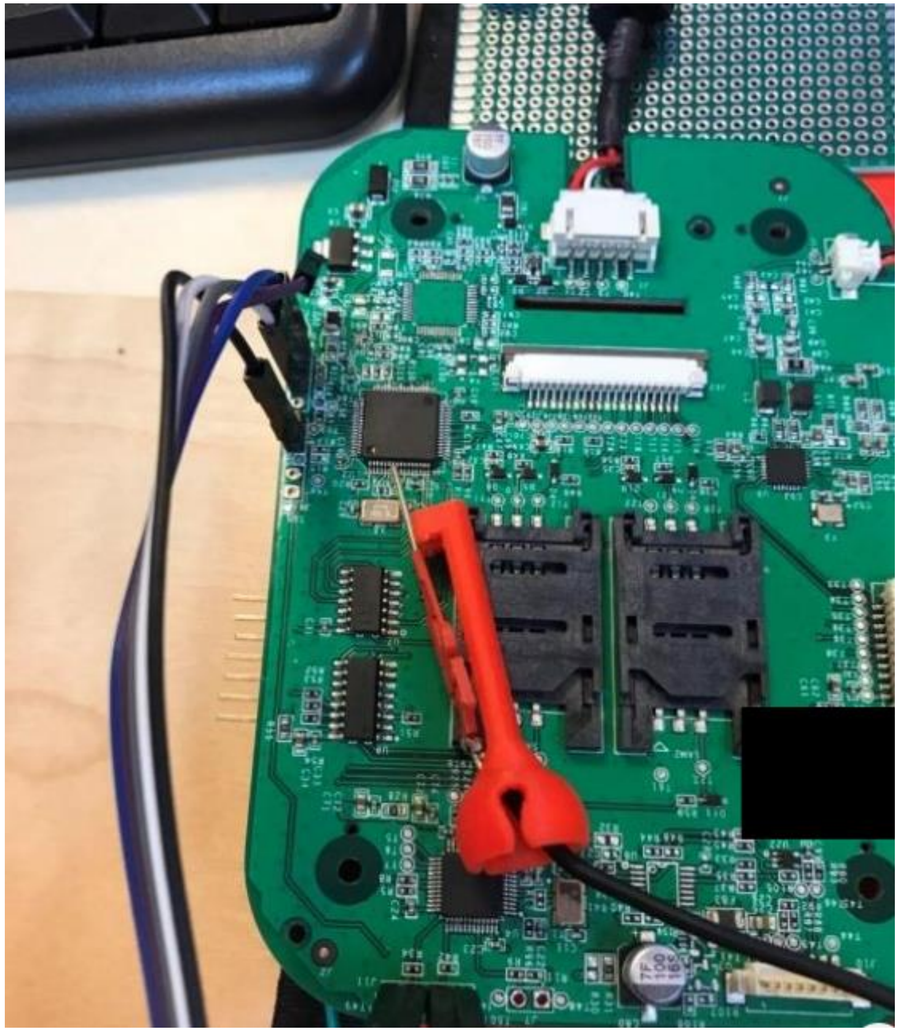
- ¿Firman mis empleados un compromiso de confidencialidad? ¿Background check?
- Están adecuadamente configurados los permisos? ¿Los reviso?
- ¿Hago backups? ¿Pruebo a restaurarlos?
- ¿Cambio regularmente las contraseñas?
- ¿Hay post-its con passwords?
- ¿Segmento adecuadamente mis redes?
- Entrevistas con el personal
- Rosetas de conexión expuestas
- Política de uso de productos seguros

El apasionante mundo de la auditoria de ciberseguridad

¿Qué clase de pruebas puedo esperar en mi producto?

Técnicas

- Búsqueda de vulnerabilidades públicas
- Problemas en la gestión de buffers
- Inyección de código
- Escaladas de privilegios y problemas en el control de acceso
- Problemas de deserialización
- Uso adecuado de la criptografía
- Datos sensibles expuestos (path traversal, …)
- Ingeniería inversa
- Ataques físicos
  - Extracción de firmware
  - Ataques de canales laterales
  - Inyección de faltas



El apasionante mundo de la auditoria de ciberseguridad

¿Qué clase de pruebas puedo esperar en mi producto?

No técnicas

- Documento el ciclo de vida y la gestión de las claves
- Los manuales no inducen al usuario a configuraciones inseguras
- Diseño y configuración secure-by-default
- Entrega del producto al usuario final no manipulable
- Adecuada gestión de los entornos de desarrollo y generación segura del producto final

El apasionante mundo de la auditoria de ciberseguridad

¿Qué clase de pruebas puedo esperar en mi proceso?

No técnicas

- Uso de metodologías de desarrollo seguro
- Gestión de la documentación
- Sitio de desarrollo seguro

Auditoría vs Certificación

¿Qué diferencia hay entre auditoría y certificación?

- **Certificación:** *Declaración **imparcial** de un tercero de que se ha **demostrado** el cumplimiento de los requisitos especificados por medio de un proceso de **evaluación***. ISO 17067:2013

- *Evaluación **formal** de productos, servicios y procesos por un organismo **independiente** y **acreditado** con arreglo a un **conjunto definido de criterios** y la **expedición de un certificado** que indique su conformidad. Comisión Europea*

Auditoría vs Certificación

¿Qué diferencia hay entre auditoría y certificación?

- **Certificación: Auditoría** con respecto a una **norma o estándar**, realizada por un **tercero acreditado**, que concluye con la emisión por parte de una **entidad de certificación** de un **certificado de conformidad**.

UNE Normalización Española

ISO

PCI

ENAC Entidad Nacional de Acreditación

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

SGS

AENOR

CCN centro criptológico nacional

Auditoría vs Certificación

¿Quién escribe las normas de ciberseguridad?

- Normas sectoriales o creadas por entidades privadas que quieren describir cómo se hacen las cosas que a ellos les afectan.

- Organizaciones internacionales cuyo único fin es precisamente escribir normas.

- Administraciones públicas o estados

Auditoría vs Certificación

*Compliance

Sistemas

Productos

Genéricas

Sectoriales

Auditoría vs Certificación

¿Por qué certificar?

- Requisitos legales
- Requisitos transitivos
- Diferencia competitiva

Auditoría vs Certificación

¿Demuestra una certificación que mi sistema/producto/proceso es ciberseguro?

- No, demuestra que un **tercero confiable** afirma que se cumple, con un determinado **nivel de garantía**, con **una especificación de seguridad**.

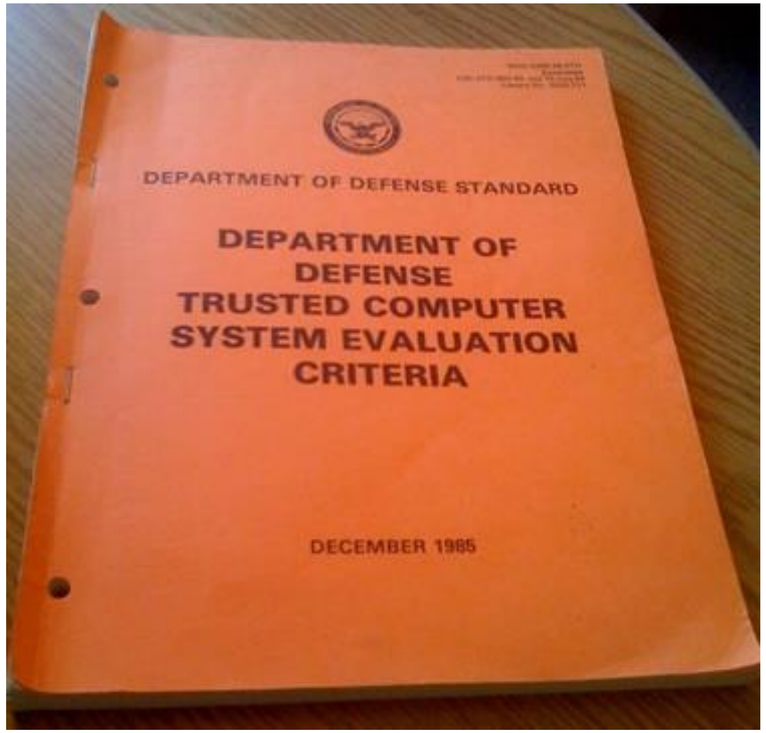
O bien

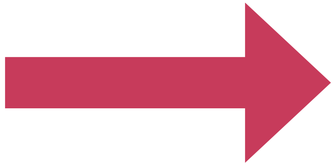
- Demuestra que la ciberseguridad está **gestionada**

CONTENIDO

No es un problema nuevo

- **80, USA:** Trusted Computer System Evaluation Criteria (TCSEC).
- **1991, Europa:** ITSEC (Information Technology Security Evaluation Criteria)
- **1993, Canada:** CTCPEC (Canadian Trusted Computer Product Evaluation Criteria)
- **1993, USA:** Federal Criteria (Draft)
- **2001, Common Criteria** (or ISO/IEC 15408)



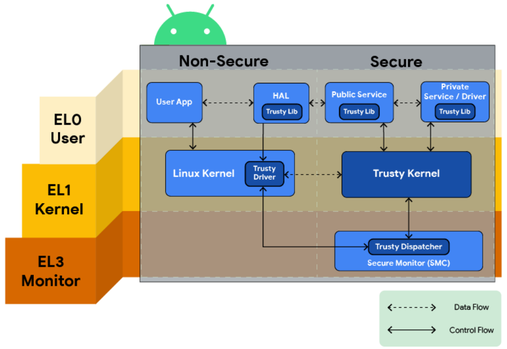


Common Criteria

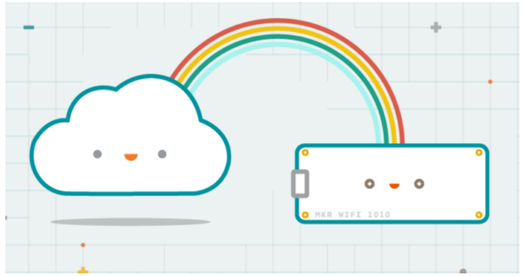
Algunos proyectos de primera categoría

Asesoramiento a uno de los mayores fabricantes de chips para certificar sus arquitecturas de seguridad para teléfonos móviles de consumo.

TrustZone®
System Security by ARM



Asesoramiento a la mayor empresa de cloud computing para sus soluciones IoT y pentesting de sus servicios.



Algunos proyectos de primera categoría

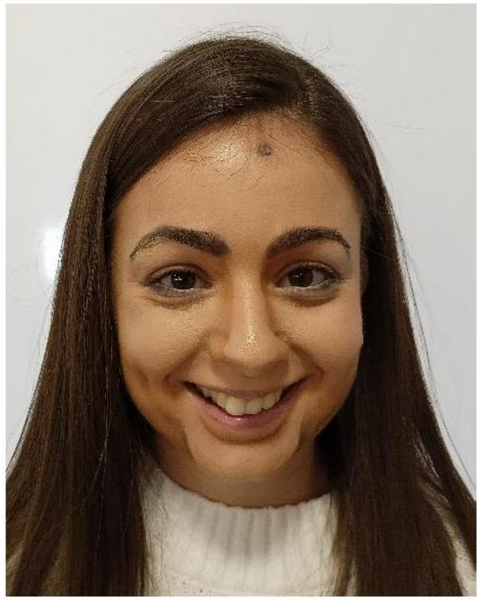
Colaboración con una de las mayores empresas de servicios públicos de España para asegurar su red de cargadores de vehículos eléctricos, realizando un pentesting de sus cargadores de vehículos eléctricos. (El pirateo de cargadores eléctricos podría suponer un problema para la red eléctrica europea, según el Foro Económico Mundial de 2019).

Algunos proyectos de primera categoría

Pruebas de penetración de software de gestión de puertos, soluciones antivirus o dispositivos cortafuegos.

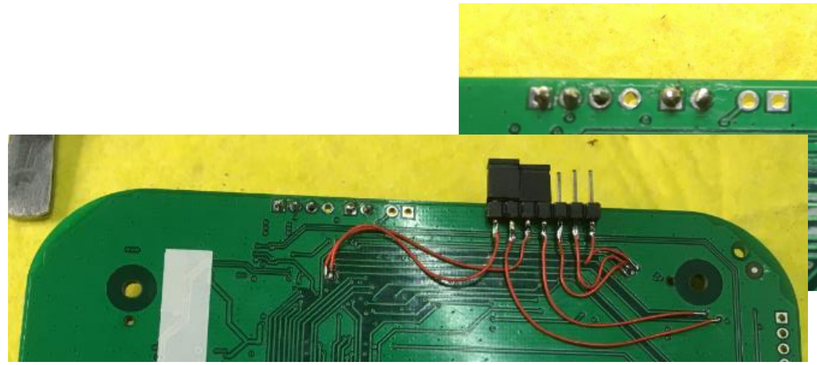
Algunos proyectos de primera categoría

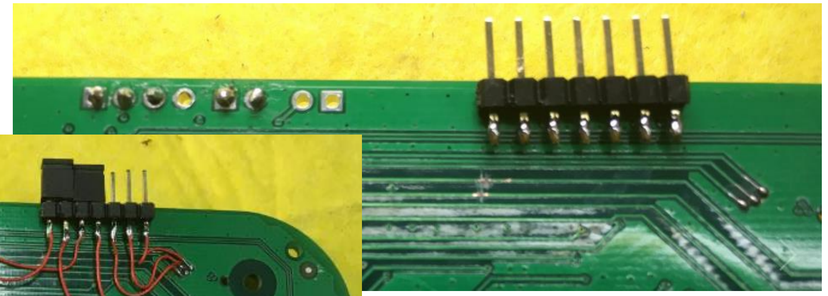
Pruebas de penetración y presentación de ataques al software de identificación por vídeo utilizado para la firma electrónica reconocida.

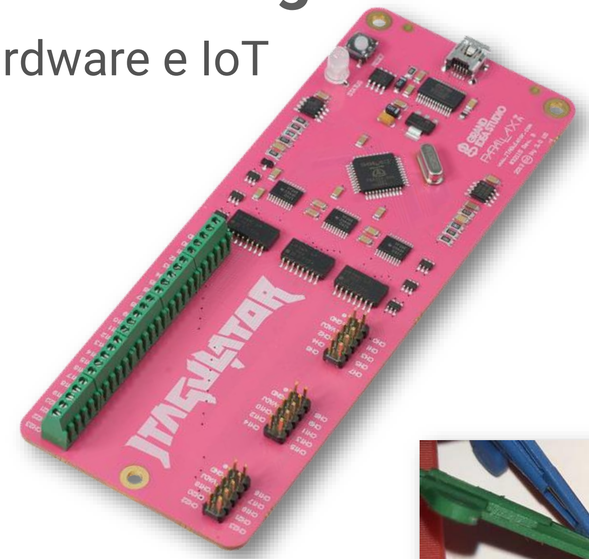


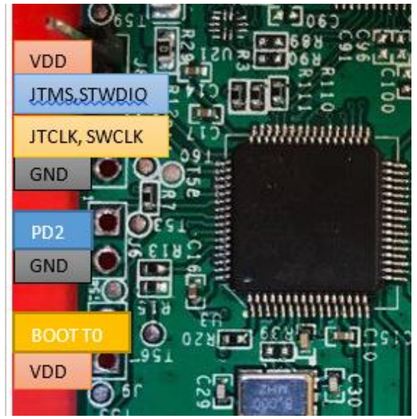
Algunos proyectos de primera categoría

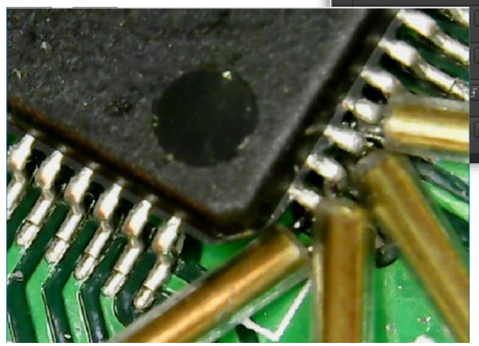
Hackeo de dispositivos hardware e IoT

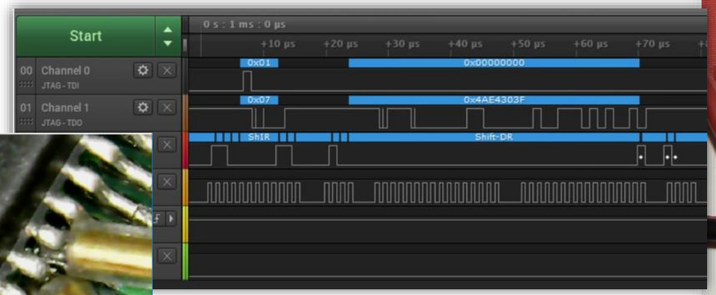


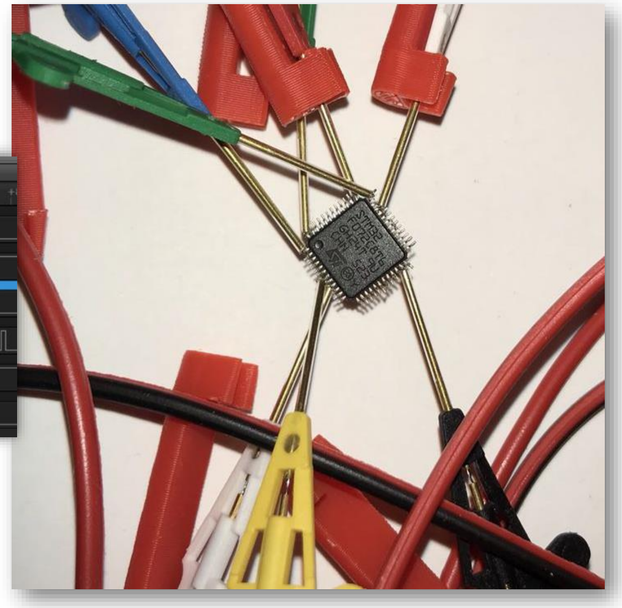






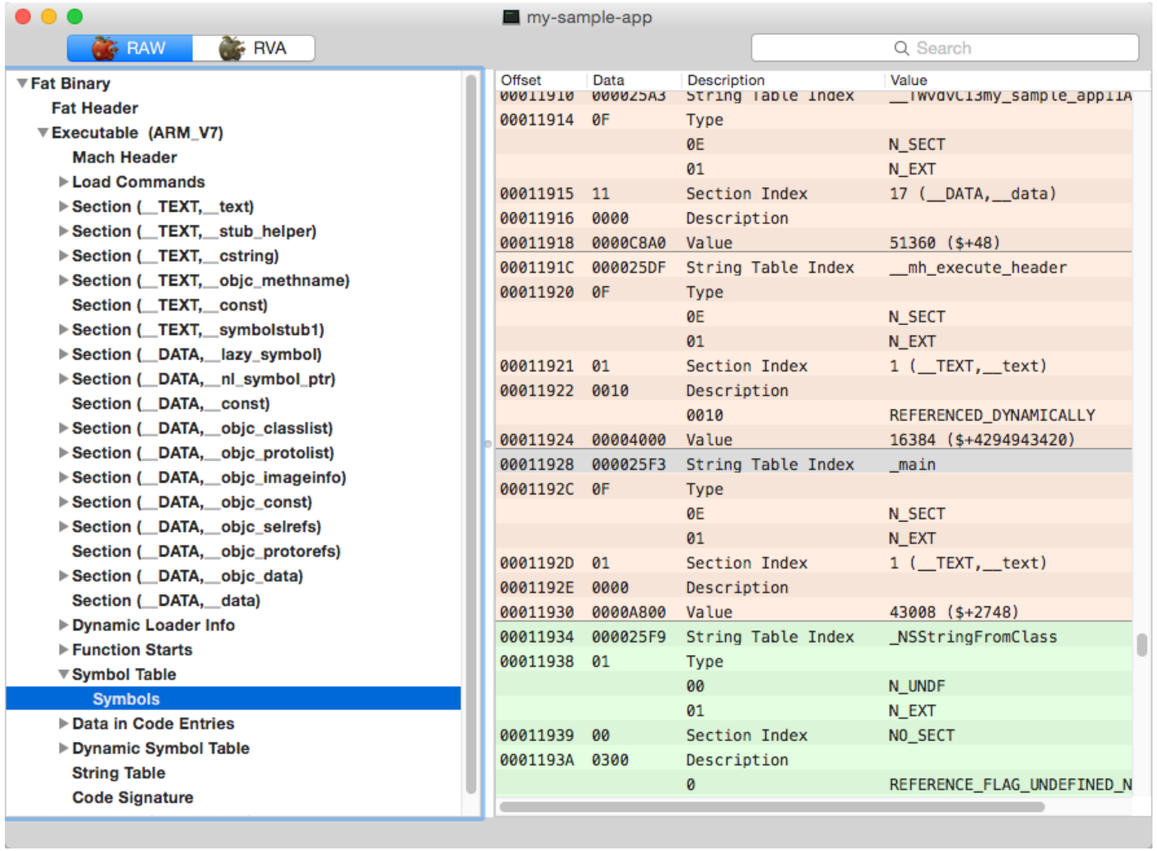






Algunos proyectos de primera categoría

Ingeniería inversa de aplicaciones móviles



jtsec SDK implementation for eID evaluation


plementation for eID evaluation
Done!


12
40
Tue, Mar 7
This device belongs to your organization

CONTENIDO

La certificación de ciberseguridad en Europa, un desafío común

Antecedentes

- 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**.
- En España, esta responsabilidad está asignada al **Centro Criptológico Nacional (CCN) desde su creación** a través del RD 421/2004 de 12 de Marzo
  - Certificación Funcional
  - Certificación Criptológica
  - Certificación TEMPEST
- Este Organismo de Certificación (OC), en lo relativo a la **certificación funcional** de la seguridad de las TI, se articula mediante el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado por **Orden PRE/2740/2007**, de 19 de septiembre.

La certificación de ciberseguridad en Europa, un desafío común

Antecedentes

- Desde entonces forma parte del acuerdo de reconocimiento mutuo **CCRA** para la norma **Common Criteria**
- En **2010** es uno de los **8 primeros países** que firma el acuerdo de reconocimiento mutuo europeo SOG-IS para Common Criteria. Hoy son 17.
- En **2018** crea **LINCE**, la cuarta metodología de evaluación europea de esfuerzo acotado. Hoy ya es la que más certificados de este tipo ha emitido en Europa.
- En la actualidad **8 laboratorios** acreditados.

CCRA

2007

Common Criteria Recognition Agreement

SOG-IS

2010

Senior Officials Group Information Systems Security

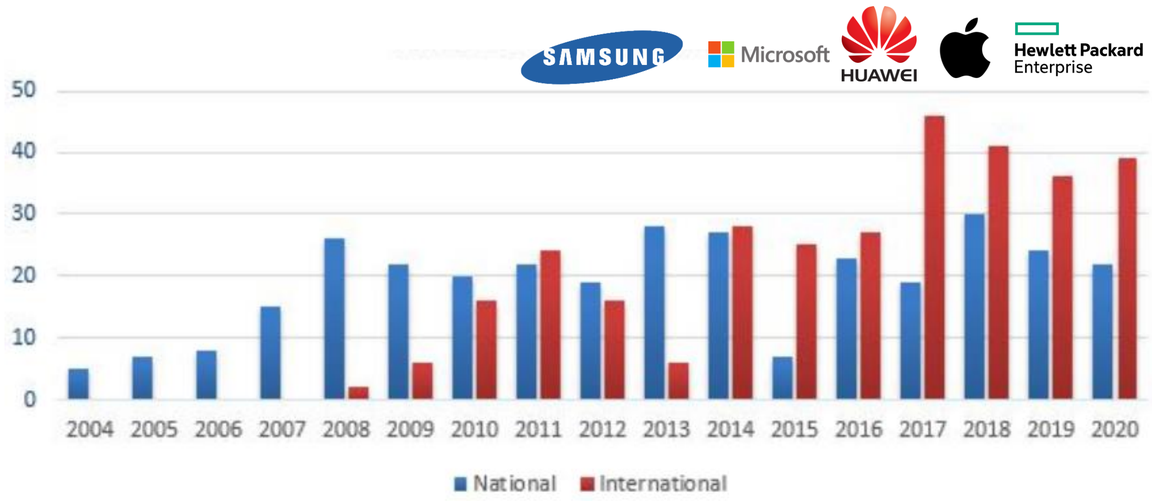
LINCE

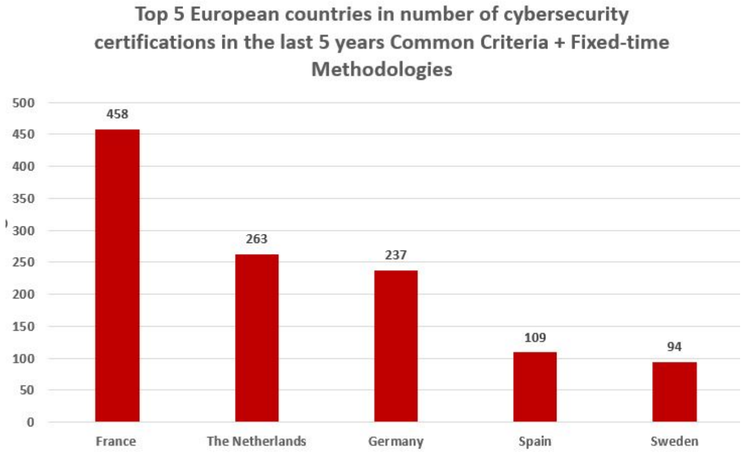
2018

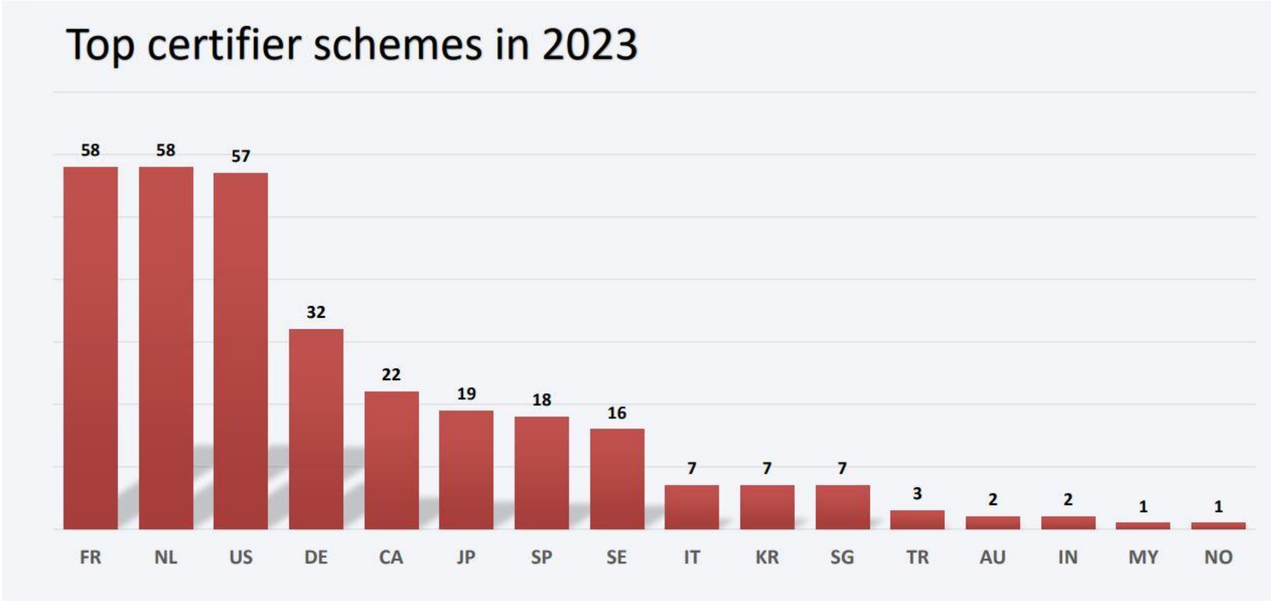
Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad

La certificación de ciberseguridad en Europa, un desafío común

Antecedentes







La certificación de ciberseguridad en Europa, un desafío común

Antecedentes

Ránking mundial. PIB, en miles de millones de dólares corrientes

	2017		2019		2021		2022	
1	EEUU	19.417,14	EEUU	21.239,30	EEUU	22.886,24	EEUU	23.760,33
2	China	11.795,30	China	13.862,97	China	16.340,87	China	17.706,63
3	Japón	4.841,22	Japón	5.085,74	Japón	5.261,88	Japón	5.368,19
4	Alemania	3.423,29	Alemania	3.617,09	Alemania	3.827,70	India	3.935,27
5	Reino Unido	2.496,76	India	2.959,67	India	3.577,13	Alemania	3.923,42
6	India	2.454,46	Reino Unido	2.607,85	Reino Unido	2.780,86	Reino Unido	2.873,37
7	Francia	2.420,44	Francia	2.562,28	Francia	2.734,10	Francia	2.815,34
8	Brasil	2.140,94	Brasil	2.340,84	Brasil	2.560,12	Brasil	2.676,27
9	Italia	1.807,43	Italia	1.879,41	Italia	1.960,25	Italia	1.993,57
10	Canadá	1.600,27	Canadá	1.719,45	Canadá	1.847,90	Canadá	1.912,81
11	Rusia	1.560,71	Rusia	1.654,09	Rusia	1.781,72	Rusia	1.840,86
12	Corea	1.498,07	Corea	1.617,44	Corea	1.756,27	Corea	1.829,01
13	Australia	1.359,72	Australia	1.497,52	Australia	1.636,25	Australia	1.709,81
14	España	1.232,44	España	1.320,08	Indonesia	1.465,84	Indonesia	1.615,56
15	Indonesia	1.020,52	Indonesia	1.206,15	España	1.411,76	España	1.451,81
16	México	987,30	México	1.094,60	México	1.217,79	México	1.283,97
17	Turquía	793,70	Turquía	876,63	Turquía	982,31	Turquía	1.031,52
18	Holanda	762,69	Holanda	807,67	Holanda	855,28	Argentina	908,33
19	Arabia Saudí	707,38	Arabia Saudí	763,00	Argentina	840,35	Holanda	876,02

Fuente: FMI

Expansión

- Por sus números, España ya es una potencia mundial en certificación de ciberseguridad.
- Si además comparamos con el PIB del país, el resultado es aun más meritorio.
- Si añadimos que el OC español está formado por un equipo de certificadores MUY inferior al de otros países, definitivamente estamos ante algo heroico.

Catálogo CPSTIC

Definición, ventajas y acceso

Art 18 Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad:
*"En la **adquisición de productos de seguridad** de las tecnologías de la información y comunicaciones que vayan a ser empleados por las Administraciones públicas se utilizarán, **de forma proporcionada a la categoría del sistema** y nivel de seguridad determinados, aquellos que tengan **certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición**, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad."*

Medidas Anexo 2: *"Componentes certificados [op.pl.5]"*
Categoría ALTA

*Se utilizarán **sistemas, productos o equipos** cuyas funcionalidades de seguridad y su nivel hayan sido **evaluados conforme a normas europeas o internacionales** y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.*

Catálogo CPSTIC

Definición, ventajas y acceso

PROBLEMA:

- Los responsables de los sistemas no saben cuáles son los productos certificados *“reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información”*

- La declaración de seguridad la escribe el fabricante, así que podría darse el caso de que la certificación no incluya todas las funcionalidades de seguridad consideradas necesarias por el CCN para un determinado tipo de producto.
  - Hay que leerla para saber el alcance > hay que entender CC

- Si el responsable de los sistemas de cada administración tiene que leerse todas las Declaraciones de Seguridad para una tipología de producto estamos escalando mal. Muy mal.

El catálogo CPSTIC

¿Qué es?

El catálogo de Productos y servicios de Seguridad TIC (CPSTIC) ofrece un listado de productos con unas garantías de seguridad contrastadas por el Centro Criptológico Nacional. Este catálogo incluye los productos **aprobados** para manejar información nacional clasificada y los productos **cualificados** de seguridad TIC para uso en el ENS.

Ventajas

1. Fácil adquisición de productos ciberseguros.
2. Evaluados por parte de un tercero confiable.
3. Disponible para todo el mundo.

Catálogo CPSTIC

Definición, ventajas y acceso

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. ENS 2022

– [op.pl.5.1]. Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (**CPSTIC**) del CCN, para seleccionar los **productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema** y aquellos que se referencien expresamente en las medidas de este real decreto.

En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19.

Una Instrucción Técnica de Seguridad detallará los criterios relativos a la adquisición de productos de seguridad.

– [op.pl.5.2] Si el sistema suministra un **servicio de seguridad** a un tercero bajo el alcance del ENS, el producto o productos que en los que se sustente dicho servicio debe superar un proceso de cualificación y ser incluido en el CPSTIC, o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento de acuerdo a lo establecido en el artículo 19.

op.pl.5	Componentes certificados	ℹ	Categoría	n.a.	aplica	aplica

Catálogo CPSTIC

Metodologías de evaluación de ciberseguridad

- Metodología ligera
- Alcance nacional
- Estándar sencillo orientado al análisis de vulnerabilidades y test de penetración
- Duración y esfuerzo acotados
- Más viable económicamente
- Accesible a PYMEs
- Su uso principal es la entrada en el catálogo
- Estándar UNE

Categoría media - básica ENS

- Metodología pesada
- Reconocida en 31 países
- Distintos niveles de garantía
- Versátil, aplicable a todo tipo de productos
- Dificultad técnica para cumplir/entender el estándar
- Mayor tiempo para su obtención
- Mayor coste económico

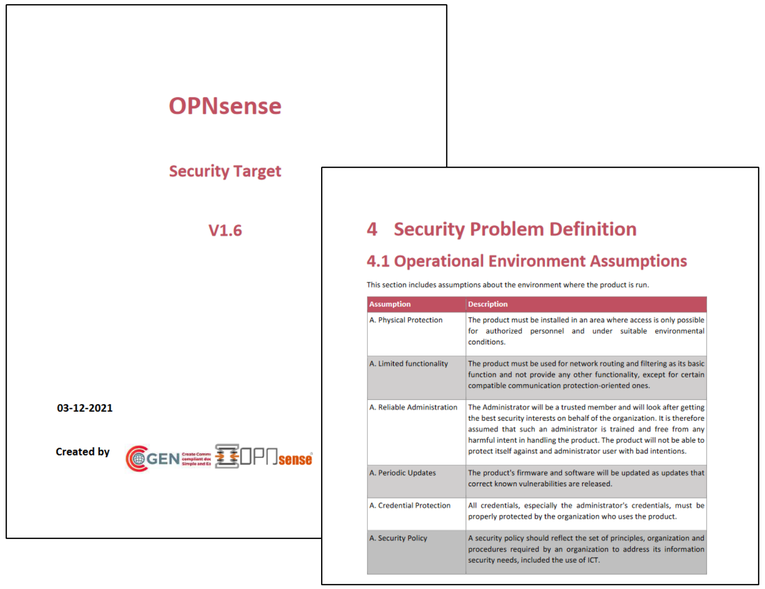
Categoría alta ENS

El catálogo CPSTIC
La declaración de seguridad

La ST (Security Target) recoge los requisitos funcionales de seguridad que implementa el TOE, así como el problema de seguridad.

Las taxonomías definen un conjunto de requisitos funcionales de seguridad. *Ej*: *La taxonomía de EDR/EPP define el siguiente requisito (uno entre tantos) que deberá cumplir todo TOE que quiera entrar en catálogo bajo la familia EDR/EPP*:

Es **crucial** definir el alcance del TOE, así como la funcionalidad que implementa él mismo y la funcionalidad que implementa el entorno operacional. Un alcance mal definido provoca varias iteraciones sobre la ST y esfuerzo perdido en evaluación, lo que conlleva a un retraso considerable de la certificación/cualificación.


OPNsense

Security Target

V1.6

03-12-2021

Created by

4 Security Problem Definition

4.1 Operational Environment Assumptions

This section includes assumptions about the environment where the product is run.

Assumption	Description
A. Physical Protection	The product must be installed in an area where access is only possible for authorized personnel and under suitable environmental conditions.
A. Limited functionality	The product must be used for network routing and filtering as its basic function and not provide any other functionality, except for certain compatible communication protection-oriented ones.
A. Reliable Administration	The Administrator will be a trusted member and will look after getting the best security interests on behalf of the organization. It is therefore assumed that such an administrator is trained and free from any harmful intent in handling the product. The product will not be able to protect itself against and administrator user with bad intentions.
A. Periodic Updates	The product's firmware and software will be updated as updates that correct known vulnerabilities are released.
A. Credential Protection	All credentials, especially the administrator's credentials, must be properly protected by the organization who uses the product.
A. Security Policy	A security policy should reflect the set of principles, organization and procedures required by an organization to address its information security needs, included the use of ICT.

38. **MAL.1** En caso de que se detecte contenido malicioso en el espacio de memoria de un proceso, se deberá interrumpir la ejecución del mismo.

El catálogo CPSTIC

Evaluación, certificación, cualificación

Evaluación

Un laboratorio independiente y acreditado verifica si un producto cumple la funcionalidad de seguridad declarada en un tiempo y esfuerzo acotados.

Certificación

El Organismo de Certificación emite un certificado de acuerdo a la funcionalidad de seguridad declarada por el fabricante.

Cualificación

Se ha superado una certificación de acuerdo a la funcionalidad de seguridad requerida por CCN.

LINCE, ENECSTI, CPSTIC y otras hierbas

¿Quién es quién?

OC-CCN

1 autoriza

Laboratorio acreditado

Certificación Nacional Esencial de Seguridad CCN

COMMON CRITERIA

3 evalúa

4 es incluido

PRODUCTO SEGURIDAD TIC ens CATEGORÍA ALTA CCN CUALIFICADO

PRODUCTO SEGURIDAD TIC ens CATEGORÍA MEDIA CCN CUALIFICADO

PRODUCTO STIC APROBADO CCN Centro Criptológico Nacional INFORMACION CLASIFICADA

cpSTIC

Catálogo de Productos y Servicios STIC

2 define requisitos de seguridad

CONTENIDO

El framework europeo de certificación y los nuevos esquemas

GDPR

2016

Relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos.

Directiva NIS

2017

Relativa a medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión

eIDAS

2016

Regula la identificación electrónica y establece unas pautas para los servicios de confianza relativos a las transacciones electrónicas.

CSA

2019

Incrementar la confianza de los usuarios respecto a los dispositivos conectados y fortalecer la industria europea de ciberseguridad.

El framework europeo de certificación y los nuevos esquemas

enisa
European Network and Information Security Agency

- **enisa como Agencia Europea de Ciberseguridad**
- **Creación de un marco europeo de certificación**
  - Incrementar la ciberseguridad dentro de la Unión Europea
  - Emitir certificados de ciberseguridad reconocidos en toda Europa
  - Mejorar las condiciones del mercado interno
    - La UE es importador neto en ciberseguridad, mientras que sus principales competidores, Estados Unidos, China, India y Japón, son exportadores netos.
  - Incrementar la competitividad y crecimiento de las compañías europeas
    - Estándares de Ciberseguridad de calidad
    - Minimizar el coste de las certificaciones

FOLLOW ENISA!

enisaeuagency

european-union-agency-for-cybersecurity-enisa

@enisa_eu

SUPPORTS EU Laws

CYBER RESILIENCE ACT, NETWORK AND INFORMATION SECURITY DIRECTIVE, REGULATION ON ELECTRONIC IDENTIFICATION AND TRUST SERVICES, EU DIGITAL IDENTITY WALLET

enisa

TOGETHER WITH:
- MEMBER STATES
- EUROPEAN CYBERSECURITY CERTIFICATION GROUP
- STAKEHOLDER CYBERSECURITY CERTIFICATION GROUP
- AD HOC WORKING GROUP

WRITES DRAFT CERTIFICATION SCHEMES WITH 3 LEVELS OF ASSURANCE

EU COMMISSION

TRANSFORMS THEM INTO:

IMPLEMENTING ACTS

SUPPORTED BY GUIDANCE DOCUMENTS

PROVIDES GUIDANCE

VULNERABILITY HANDLING ON CERTIFIED SOLUTION

RESOLVE

EU CYBERSECURITY CERTIFICATION

KEY ACTORS AND THEIR ROLE

NCCAs NATIONAL CYBERSECURITY CERTIFICATION AUTHORITIES DESIGNATED IN EACH MEMBER STATE

SUPERVISE THE IMPLEMENTATION

PEER EVALUATIONS

PROVIDERS OF ICT SOLUTIONS

CERTIFICATES DELIVERED

Certify

AND NOTIFY CABs

CABs CONFORMITY ASSESSMENT BODIES

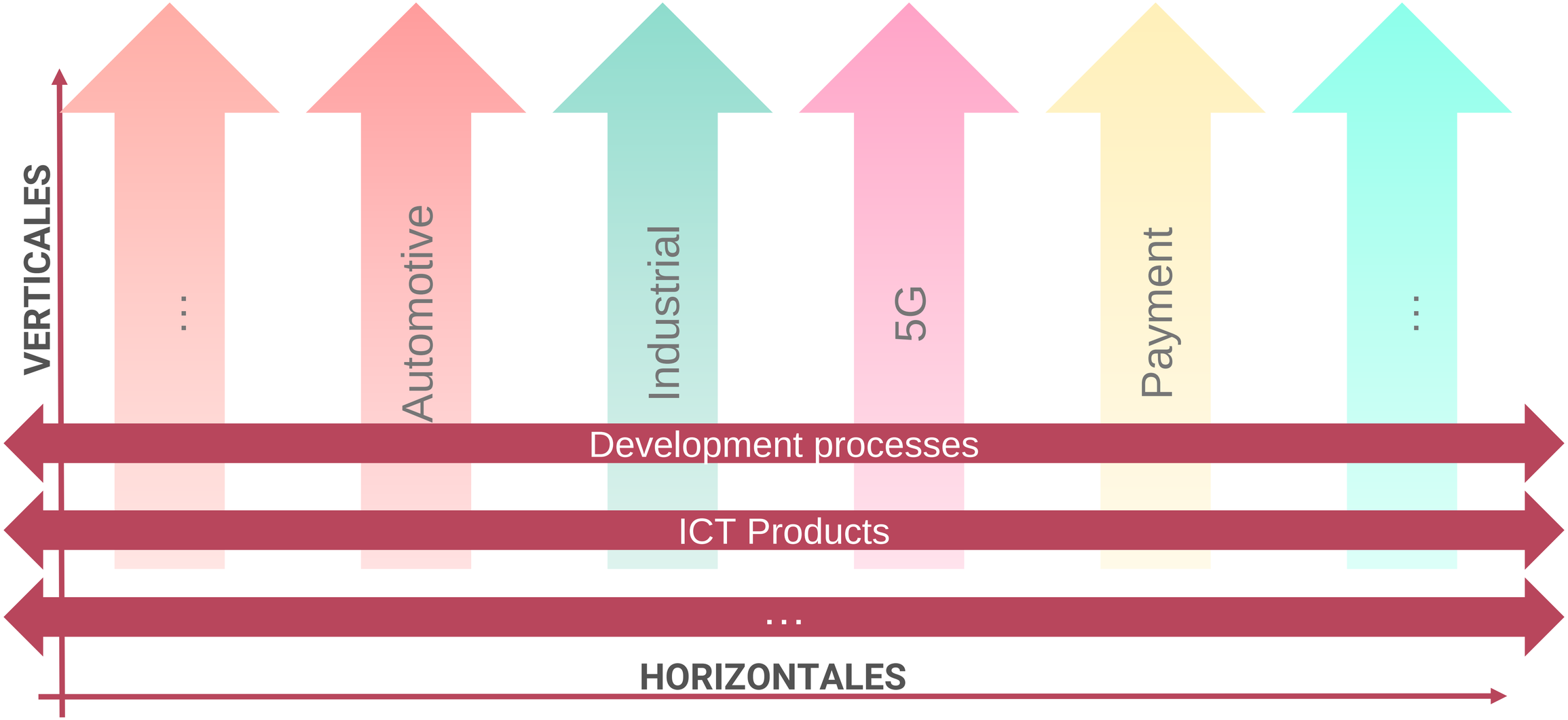
ACCREDIT CABs

NABs NATIONAL ACCREDITATION BODIES

PEER EVALUATIONS

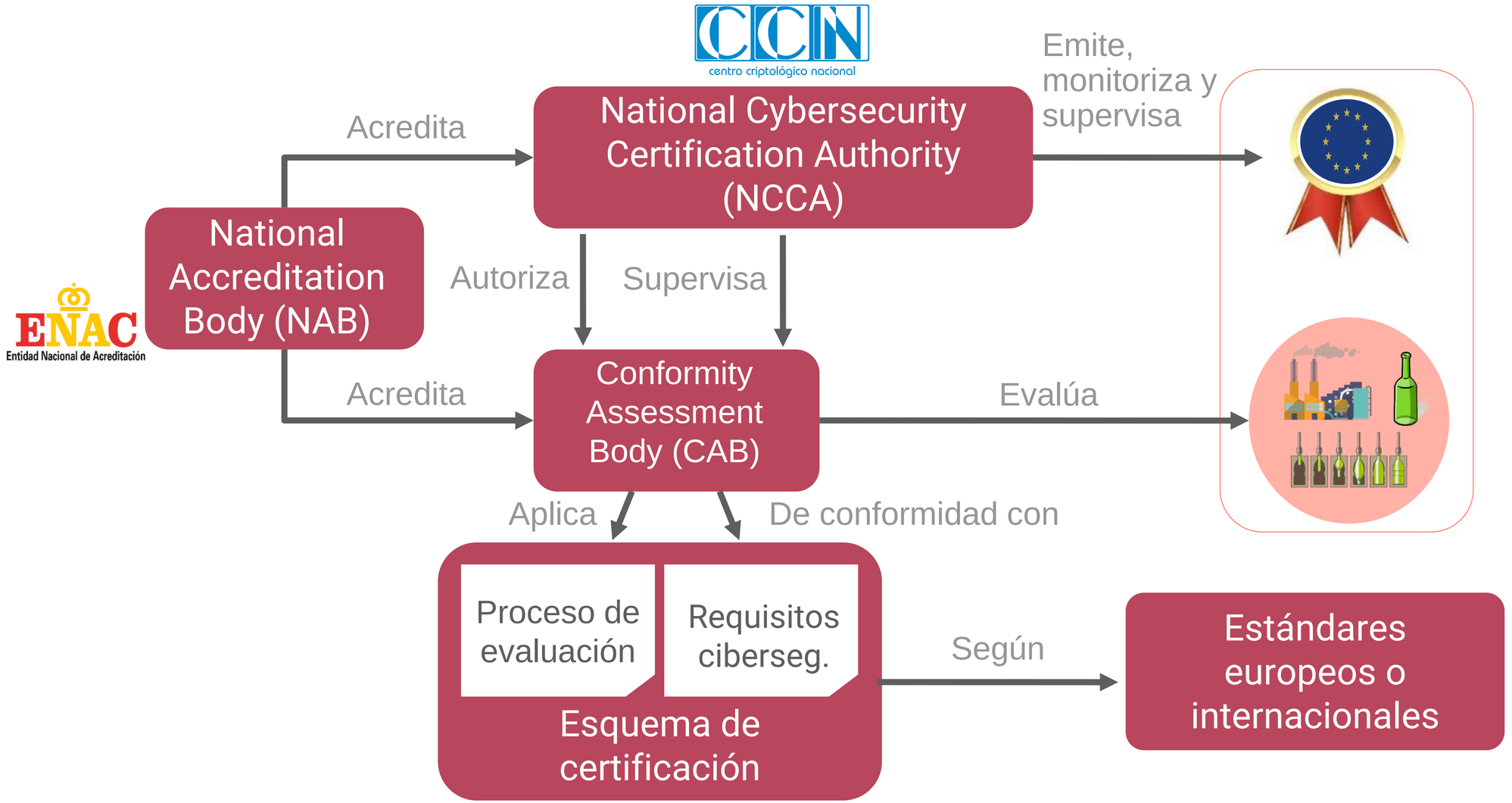
enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

El framework europeo de certificación y los nuevos esquemas



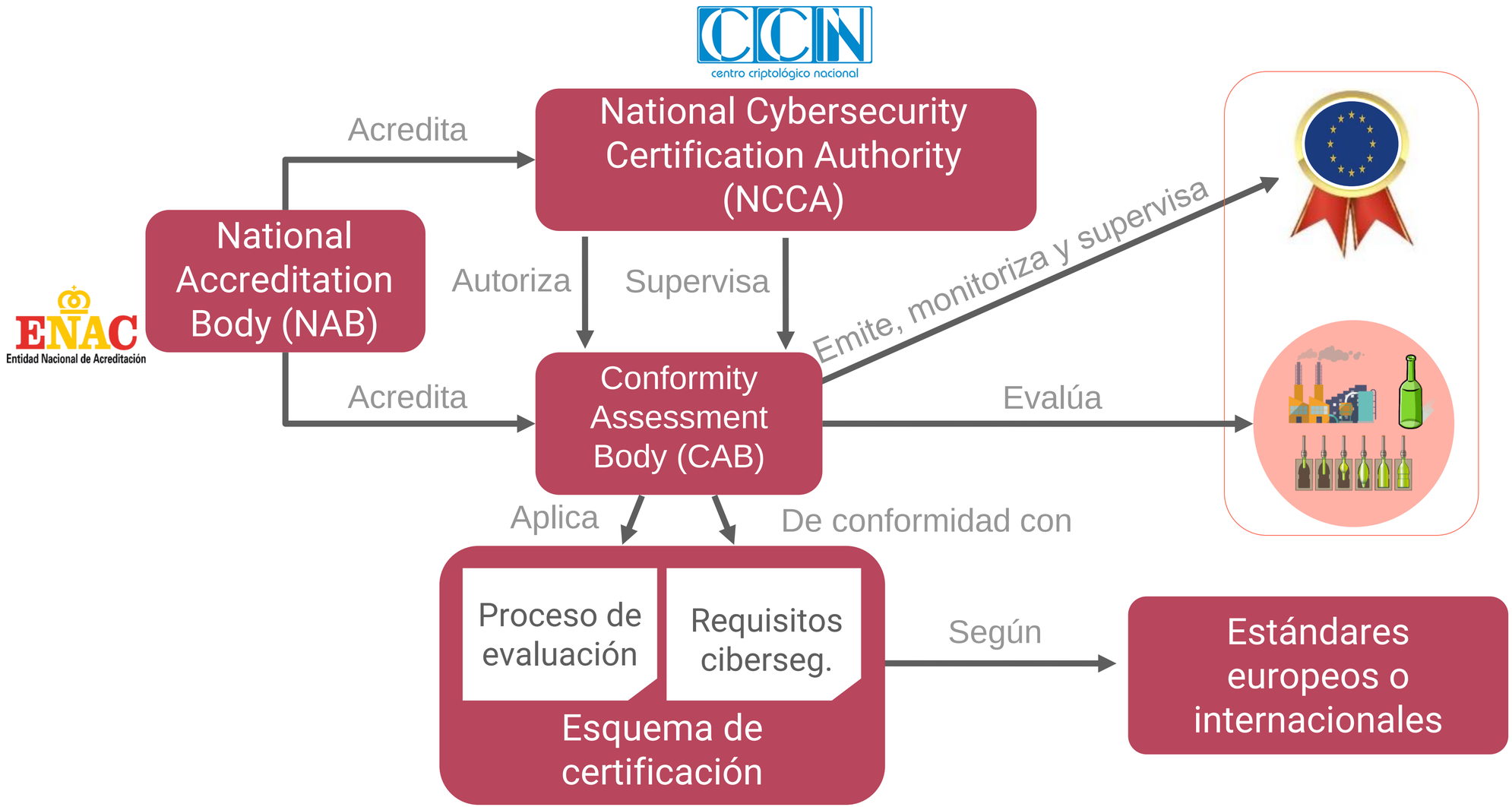
El framework europeo de certificación y los nuevos esquemas

Nivel de garantía: alto



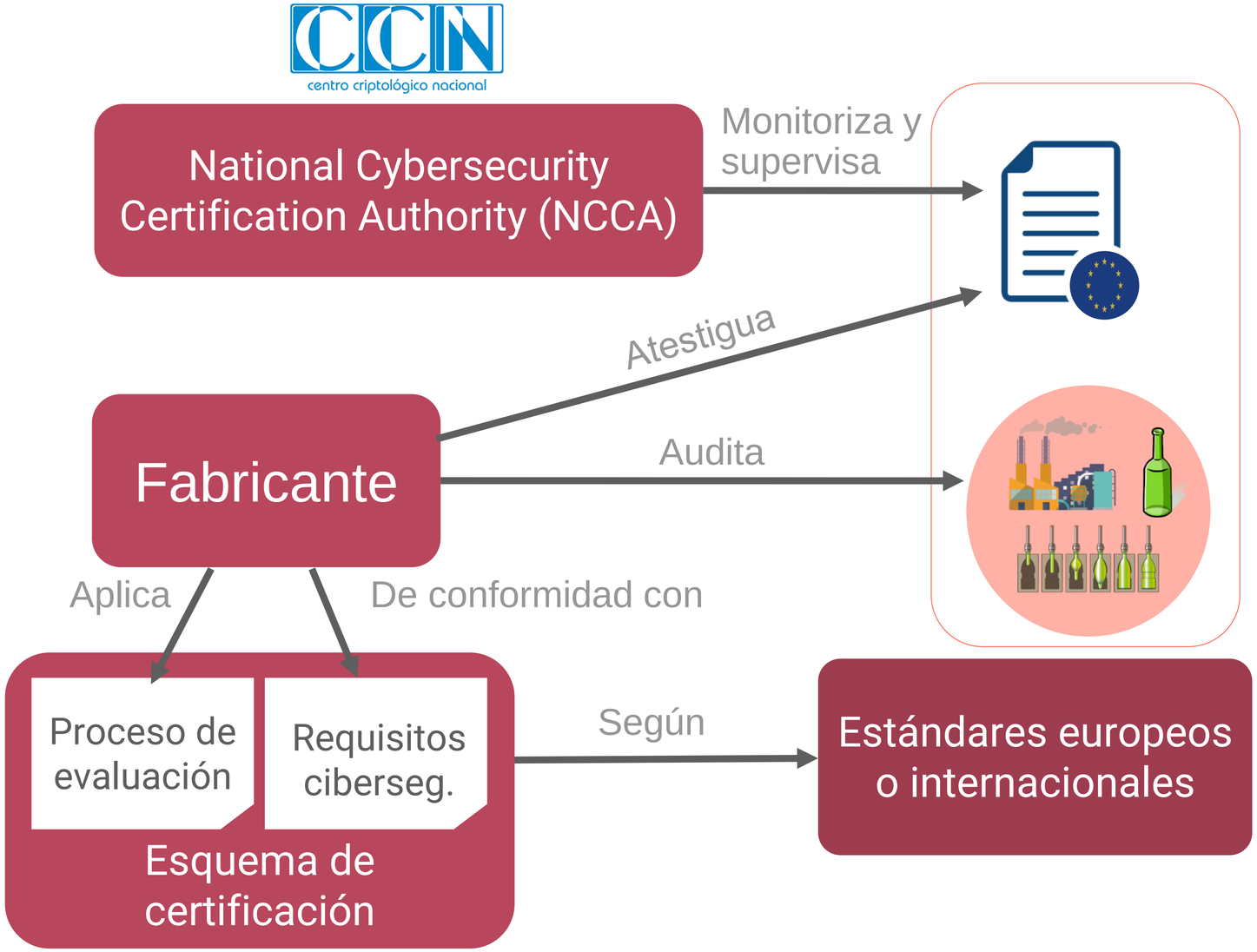
El framework europeo de certificación y los nuevos esquemas

Nivel de garantía: substancial



El framework europeo de certificación y los nuevos esquemas

Nivel de garantía: básico



El framework europeo de certificación y los nuevos esquemas

Nivel	¿Qué se prueba?	Objetivo	Tipo de evaluación minima	¿Quién hace las pruebas?	¿Quién emite el certificado?
High	Cumplimiento y robustez	Preservar la soberanía, proteger al ciudadano y a la industria de organizaciones criminales	Pruebas de penetración Ataques State-of-the art	CAB-ITSEF	NCCA
Substantial	Cumplimiento y robustez	Prevenir ataques escalables en dispositivos de coste medio/alto	Ausencia de vulnerabilidades públicas Pruebas de conformidad	CAB-ITSEF	CAB-CB
Basic	Cumplimiento	Prevenir ataques masivos en dispositivos de bajo coste	Revisión de documentación técnica	CAB-ITSEF	CAB-CB
			Auto-evaluación	Fabricante	N/A. Declaración de conformidad

El framework europeo de certificación y los nuevos esquemas

Obligaciones para los fabricantes

- Repositorio de vulnerabilidades públicas y dirección de contacto
- Periodo de soporte: durante cuanto tiempo se espera proveer parches.
- Notificar dependencias

Gestión de no conformidades

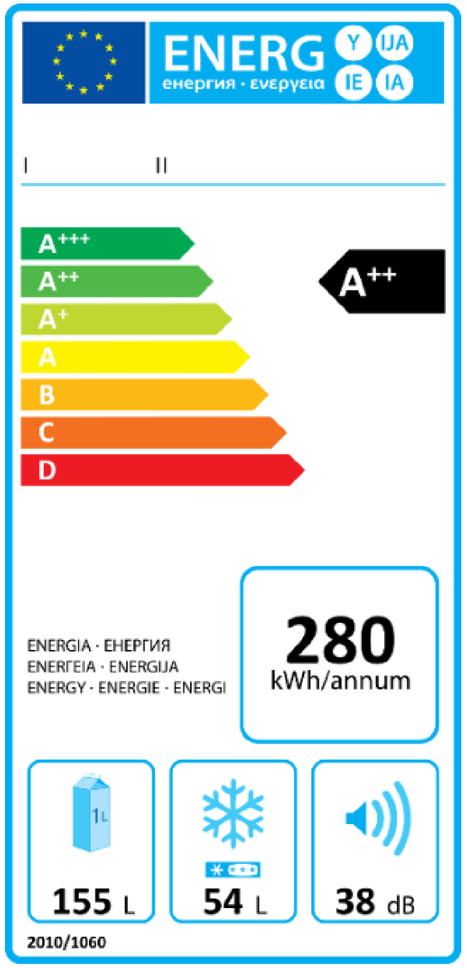
- E.g. Uso ilegítimo del certificado, no proporcionar parches de manera efectiva
- ¡Responsabilidad legal! Potenciales multas a fabricantes o CABs

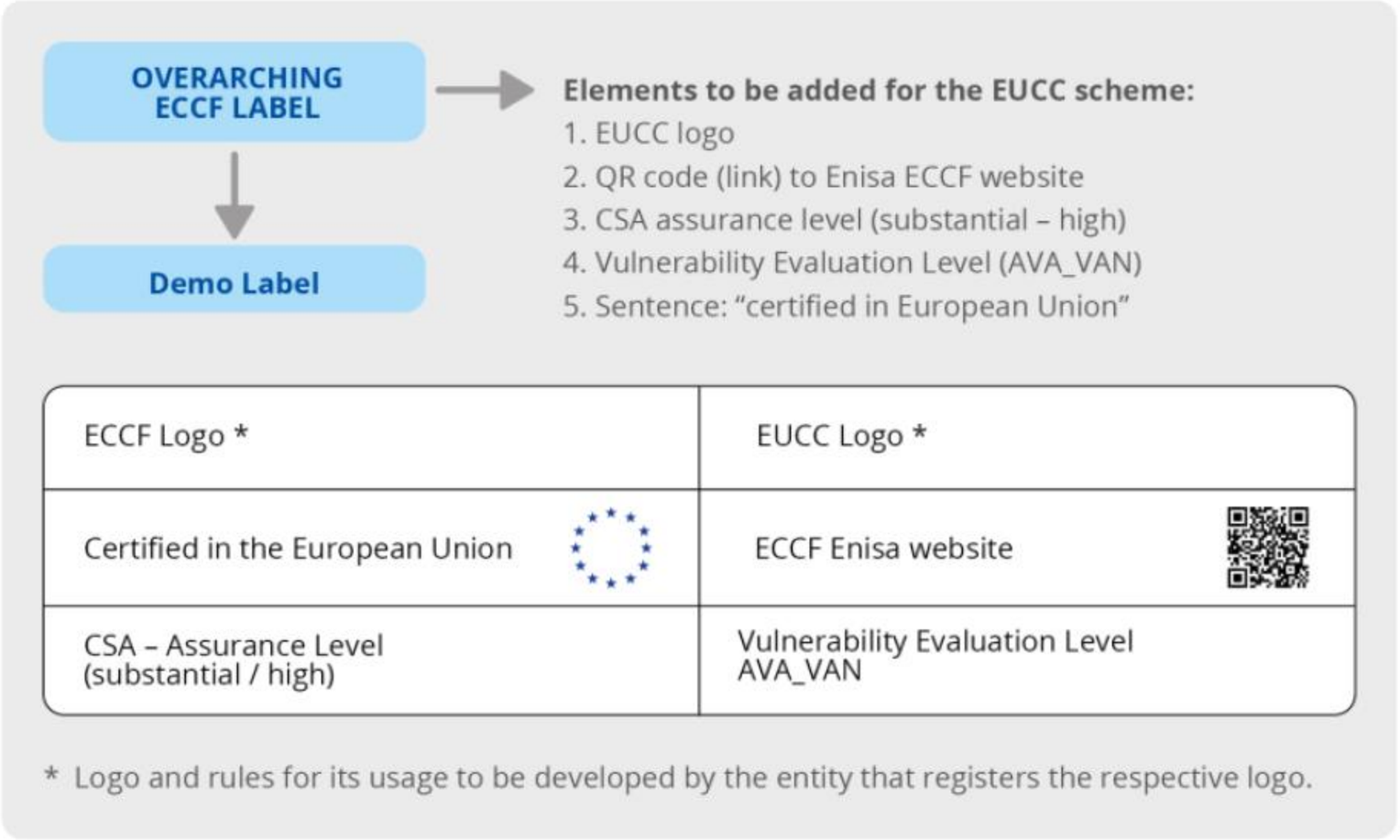
Monitorización del cumplimiento

- Análisis del panorama de amenazas
- Potencialmente repetir evaluaciones

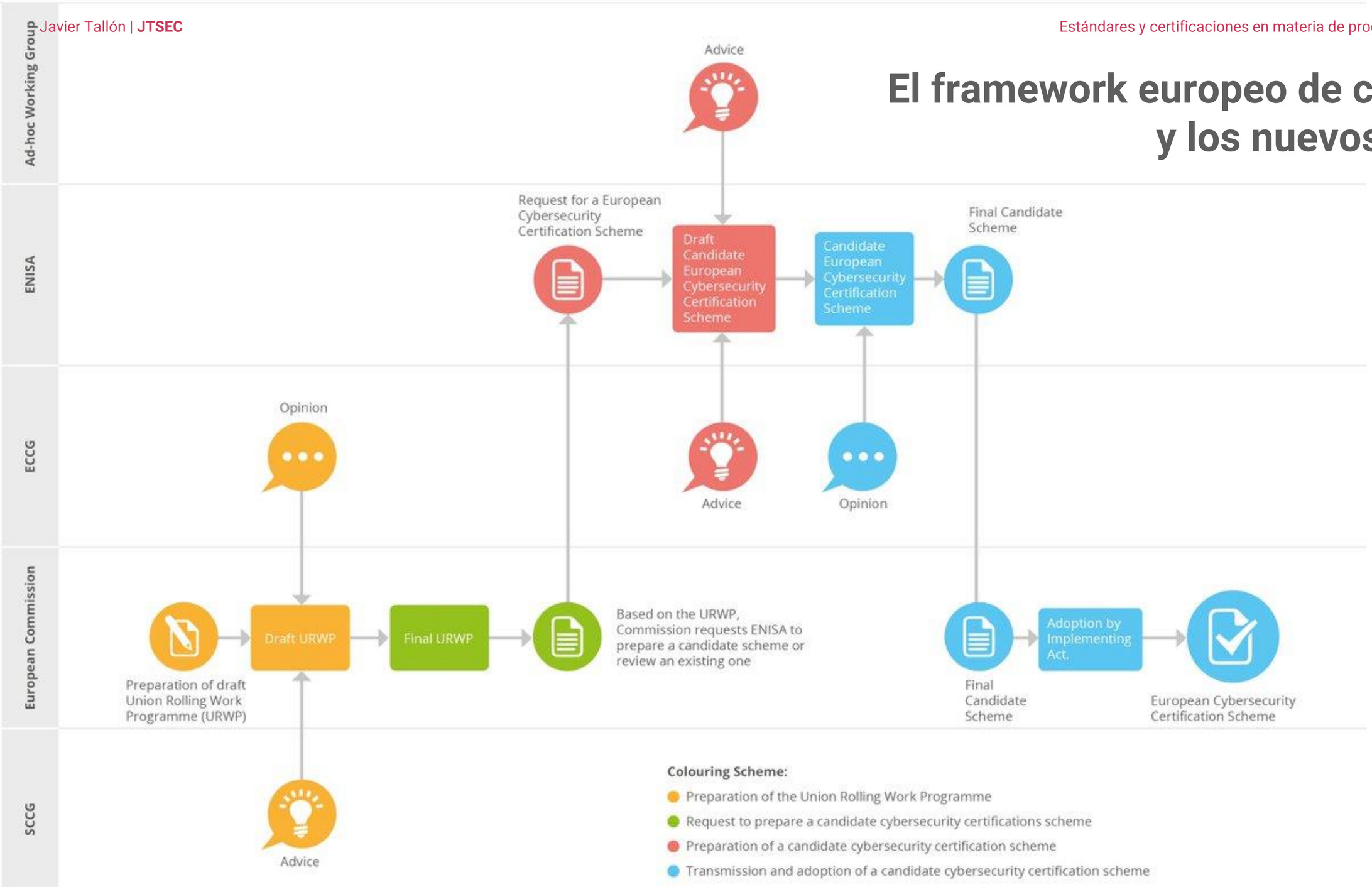
La certificación sigue siendo voluntaria… hasta que se indique lo contrario.

El framework europeo de certificación y los nuevos esquemas





El framework europeo de certificación y los nuevos esquemas



El framework europeo de certificación y los nuevos esquemas

EUCC

- Esquema de certificación de **productos** para niveles substancial y alto
- Trasposición del **SOG-IS**: Good old Common Criteria
- **31/01/2024 Publicación del Implementing Act**
- Novedades
  - Patch Management
  - Critical Update Flow
  - ISO/IEC 15408 & ISO/IEC 18045
  - Periodo de transición de entre 1 y 2 años
  - Mayor colaboración fabricante - laboratorio

Common Criteria

El framework europeo de certificación y los nuevos esquemas

EUCS

- Esquema de certificación de **servicios** para niveles básico, substancial y alto
- No self-assessment
- Se lanza Adhoc WG en Marzo de 2020
- **Afectará a todos los proveedores de servicios cloud**
- **¿Voluntario? → NIS2**
- **Se filtró y se lió**

EL PROBLEMA DE LA SOBERANÍA

Los requisitos de soberanía son necesarios para *"ofrecer garantías sobre la independencia de la legislación de fuera de la UE"*

NIVEL HIGH: *"operados únicamente por empresas de la UE, sin que ninguna entidad de fuera de la UE tenga un control efectivo sobre el CSP [proveedor de servicios en la nube], para mitigar el riesgo de que poderes injerencistas de fuera de la UE socaven la normativa, las normas y los valores de la UE"*.

POSIBLE SOLUCIÓN

HIGH: localizar todas las actividades de tratamiento de datos en la UE.

HIGH+: todas las actividades de tratamiento de datos tengan lugar en la UE. Enumerar todas las actividades de apoyo realizadas fuera de Europa.

El framework europeo de certificación y los nuevos esquemas

Nuevos esquemas

- **Componentes Industriales (IACS)**
  - Los sistemas de control industrial son construidos como la integración de múltiples y dispares componentes hardware/software
  - Asegurar IACS asegurando sus componentes
  - Hay una propuesta de ERNCIP (European Reference Network for Critical Infrastructure Protection), dependiente de la Comisión Europea
  - Potenciales metodologías: IEC 62443 & Lightweight (e.g. Lince)
  - Contempla self-assessment

- **IoT**
  - ¿Qué es IoT?
  - Depende del uso > Esquema genérico
  - Potenciales metodologías: ETSI EN 303 645

- **+ 5G**

URWP

Q1 2021

El framework europeo de certificación y los nuevos esquemas

EU5G

- Servicios críticos dependerán del 5G
- Contemplado desde la publicación de la EU Toolbox
- Alcance:
  - ➢ Suministro y despliegue de equipos de red 5G
  - ➢ Gestión de las identidades de los abonados
  - ➢ Provisión remota de SIM
  - ➢ Autenticación 5G (incluida la itinerancia)
  - ➢ Servicios de conectividad de abonados

- GSMA NESAS

El framework europeo de certificación y los nuevos esquemas

Nuevos esquemas

- **Posibles solicitudes de certificación europea de ciberseguridad vinculadas a la evolución legislativa**
  - European Digital Identity Wallets
  - Managed security services: servicios de respuesta a incidentes, pruebas de penetración y auditoría y consultoría de ciberseguridad

- **Otros ámbitos de reflexión**
  - CRA →
  - ➢ ¿Necesitamos IoT / IACS?
  - ➢ Procesos de desarrollo: Identificar/desarrollar estándarles
  - Criptografía: harmonizar su uso. Post-quantum. ¿Es necesario un esquema?
  - Fixed time evaluation

- **+ IA**
  - estudio de viabilidad sobre los requisitos de certificación de ciberseguridad de la UE en materia de IA

URWP

Q1 2024

El framework europeo de certificación y los nuevos esquemas

Potenciales nuevos esquemas a futuro

European Commission

Medical Devices Regulation

EU MDR

UNECE WP.29

CONTENIDO

Certificación de ciberseguridad de la UE y legislación de la UE

Evolución del paisaje sobre ciberseguridad

Nuevas leyes de la UE con requisitos de ciberseguridad referentes a la certificación de ciberseguridad de la UE:

- **CRA, NIS2, AI Act, Chips Act, eIDAS2, Solidarity Act**

Impacto para la certificación europea de ciberseguridad

La ley de ciberresiliencia (CRA)

(TIC) **Productos con elementos digitales** que entran en el mercado de la **UE** (independientemente del origen)

Marcado CE → Necesidad de ser seguro (safe), proteger la salud

+ CRA → Necesidad de cumplir los **requisitos esenciales de ciberseguridad** (anexo I)

- **Durante el ciclo de vida del producto** o como *máximo* 5 años después de haber sido introducido en el mercado
- Cumplimiento supervisado por **las autoridades de vigilancia del mercado** (nombradas por los Estados Miembro) competencias de investigación, retirada de productos del mercado y sistema de sanciones
- Productos con elementos digitales **divididos en clases de riesgos, evaluados de manera diferente**
- **Aprobada el 12 de marzo de 2024**
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

Alcance de CRA

Productos con elementos digitales

- ✚ **Productos y componentes de hardware** comercializados en el mercado por separado, como ordenadores portátiles teléfonos móviles, equipos de red o CPUs
- ✚ **Productos y componentes de software** comercializados en el mercado por separado, como sistemas procesamiento de textos, juegos o aplicaciones apps

ⓘ La definición de "**productos con elementos digitales**" incluye también la parte de **procesamiento de datos a distancia (cloud).**

No cubiertos

- ✖ **Proyectos no comerciales, incluidos los open source** (en la medida en que no forme parte de una actividad comercial)
- ✖ **Servicios, en particular SaaS** - *cubierto por NIS2*

Exclusiones directas

- ✖ **Determinados productos suficientemente regulados en materia de ciberseguridad** (automóviles, dispositivos médicos, in vitro, equipos aeronáuticos certificados) según el nuevo y antiguo enfoque

Obligations of manufacturers

Assessment of the risks associated with a product

(1) **Product-related** essential requirements (Annex I, Section 1)
(2) **Vulnerability handling** essential requirements (Annex 1, Section 2)
(3) **Technical file, including information and instructions** for use (Annex II + V)

Conformity assessment, CE marking, EU Declaration of Conformity (Annex IV)

Continued compliance with **vulnerability handling** essential requirements throughout the product life time (Annex I, Section 2)

Design and development phase

Maintenance phase
(5 years or across product lifetime, whichever is shorter)

Obligation to report to ENISA within 24 hours:

(1) **exploited vulnerabilities**
(2) **incidents** having an impact on the security of the product

Reporting obligations to continue

CRA

Requisitos Esenciales de Seguridad

1. **Diseñar, desarrollar y producir productos** que garanticen un **nivel adecuado de ciberseguridad basado en riesgos**

2. **Sin vulnerabilidades** explotables conocidas

3. **Realizar una evaluación de riesgos** que cubra:

    - **El producto es seguro por defecto** y tiene la posibilidad **de reset**
    - **Protección contra** el **acceso no autorizado**
    - **Protección de la confidencialidad** de los datos procesados mediante cifrado y mecanismos de última generación
    - **Protección de la integridad** de los datos procesados, comandos, programas y configuración contra manipulación, corrupción o modificación no autorizada por el usuario
    - **Procesamiento únicamente de datos pertinentes**, adecuados y limitados a lo necesario para el uso previsto → principio de minimización GDPR
    - Resiliencia ante DoS y mitigar impacto negativo en otros servicios
    - Ser diseñado, desarrollado y producido para **limitar la superficie de ataque** y las interfaces externas, para **reducir el impacto de un incidente** — mecanismos de mitigación
    - Logging
    - Comprobar que las vulnerabilidades se puedan abordar mediante **actualizaciones de seguridad** (automatizadas)

CRA

Cómo cumplir con los requisitos esenciales

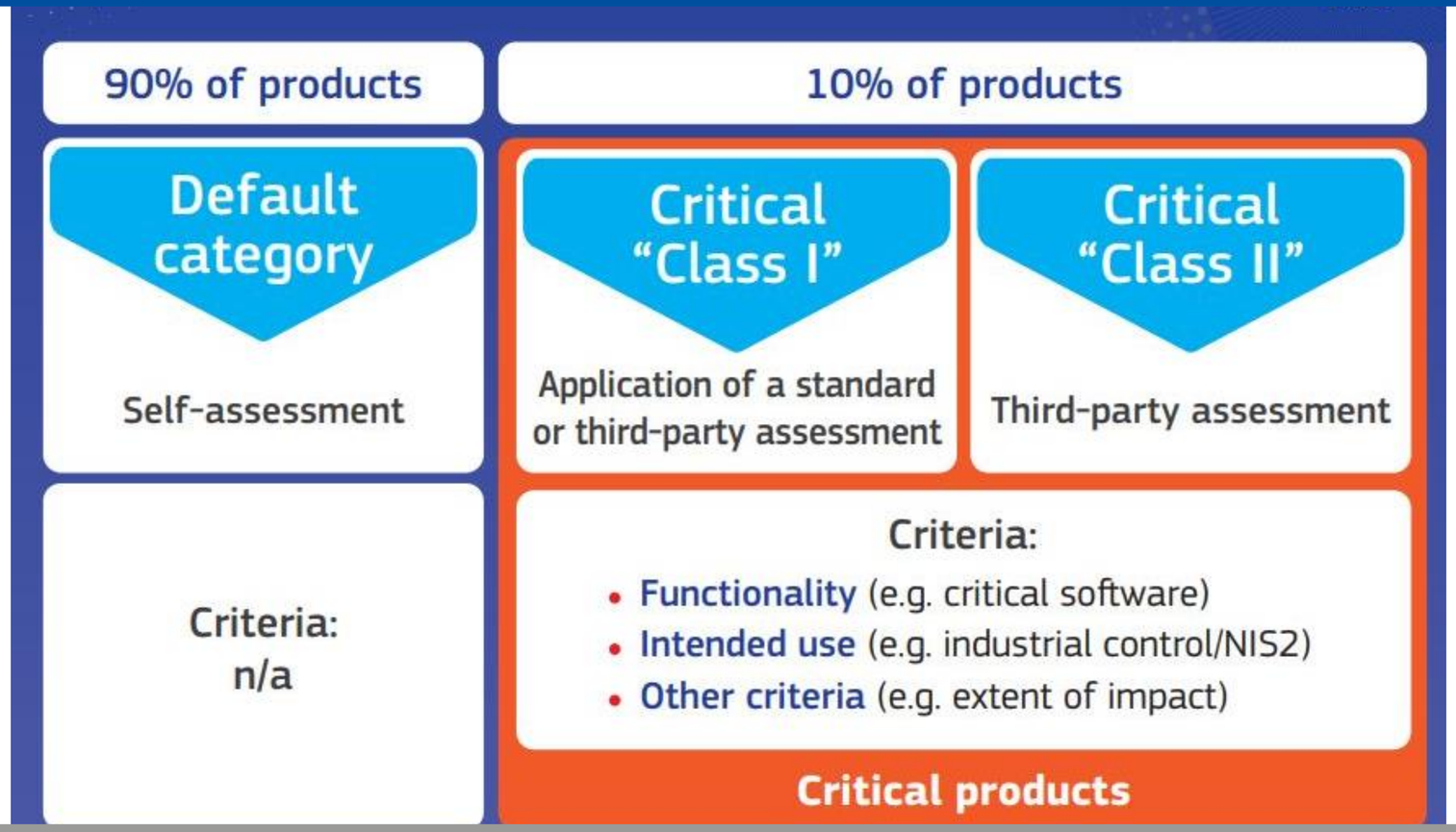
El fabricante podrá utilizar:

1. **Normas armonizadas** (publicadas en el BO de la UE)
2. **Especificaciones definidas por la Comisión** si no existe o no cumple ninguna norma armonizada (Implenting Act).
3. **Certificación de ciberseguridad de la UE:**

    - La Comisión está facultada para especificar, mediante Implementing Act, los esquemas que pueden utilizarse para la presunción de conformidad
    - La Comisión también puede especificar si un certificado de ciberseguridad de la UE elimina la obligación de realizar una evaluación de terceros

CRA

Requisitos esenciales de ciberseguridad



Productos altamente críticos
(Párrafo 5 del artículo 6)

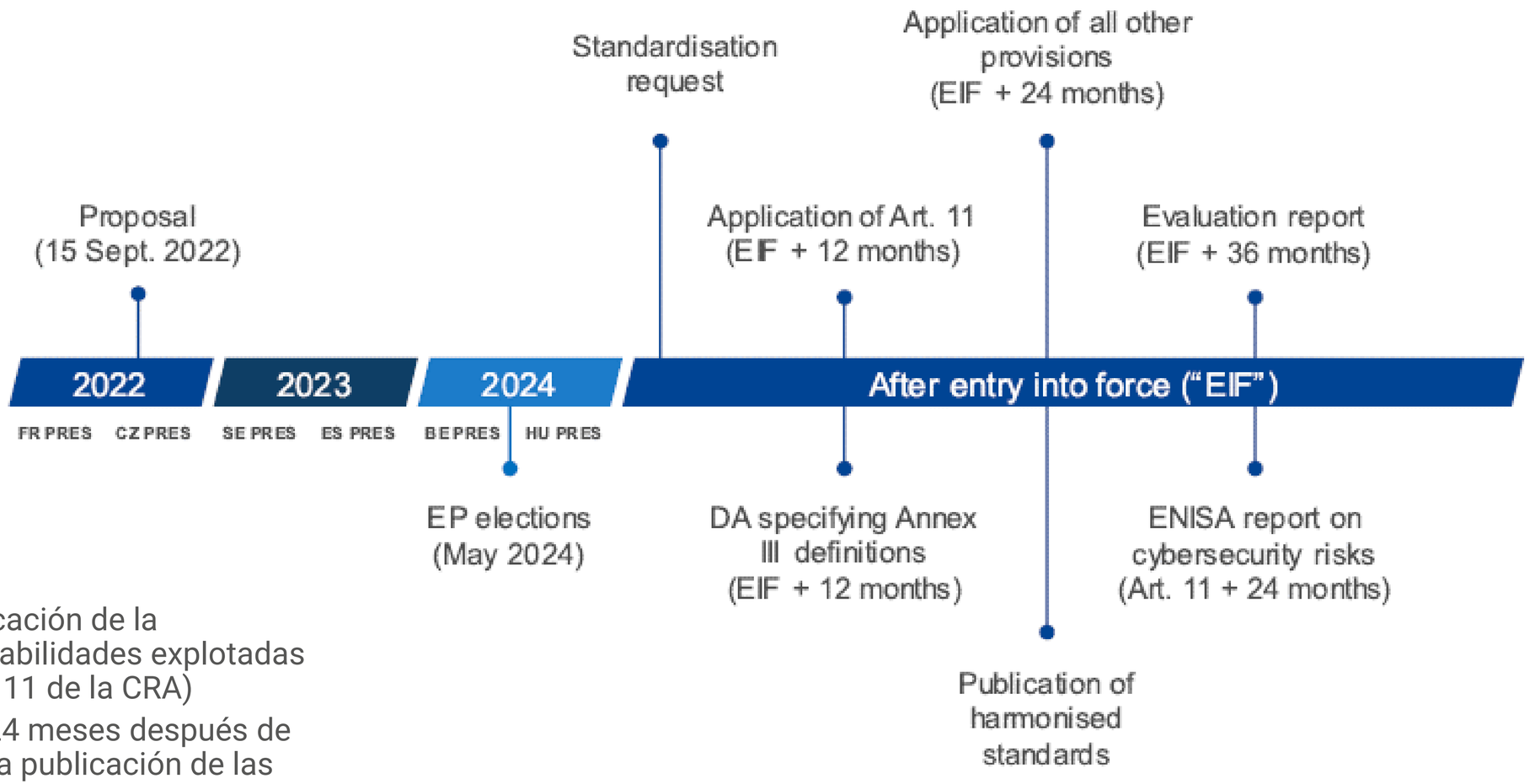
- Entidades NIS2
- Resiliencia de la cadena de suministro ante eventos disruptivos

Certificación de ciberseguridad obligatoria

Especificados (y modificables) a través de actos delegados

CRA

¿Cuáles son los plazos para la CRA?



- Comienza con la aplicación de la notificación de vulnerabilidades explotadas activamente (artículo 11 de la CRA)
- Otras disposiciones 24 meses después de la entrada en vigor y la publicación de las normas armonizadas
- Los actos delegados de la UE ampliarán y especificarán más las normas

CRA

CSA vs CRA

CSA — Certificación

- **Ciclo de vida a largo plazo garantizado**
- **Composición de las certificaciones**
- **Niveles de garantía basados en el riesgo y los** correspondientes requisitos de seguridad cibernética (con upgrades / downgrades)
- **Horizontal y sectorial**
- **Acreditación y Autorización** (alta) de CABs
- **Procedimientos de reclamación para todos los agentes** (CAB & NCCA) y recursos legales
- Base de datos **central de certificación de la UE** ENISA
- El Reglamento de aplicación tiene una cláusula de fallback: cláusula de reparación si los procedimientos no funcionan.
- Deficiencias de un esquema: solicitud de revisión del ECCG o de la Comisión ex art 48, apartado 2, de la CSA
- No hay seguridad explícita de la cadena de suministro y minimización de datos
- Notificación de nuevas vulnerabilidades desconocidas

CRA — Declaración de conformidad/certificado de evaluación

- **Ciclo de vida a corto plazo** -máximo 5 años
- **Sin sistema de composición**
- **Requisitos «estáticos» pero genéricos, evaluación de la conformidad basada en el riesgo**
- **Horizontal**
- **No se obliga a acreditar**
- **Procedimientos de reclamación: no se describe explícitamente en CRA (¿**regulado por el uso de estándares harmonizados?)
- **Descentralizado: los organismos nofiticados** disponen de la información de certificación (y el estado)
- **Incumplimiento** atribuido al sistema de deficiencia → Enmienda de la Comisión/derogación del Implementign Act que describe la presunción de conformidad (artículo 18, apartado 4, del CRA)
- Seguridad de la cadena de suministro: SBOM y minimización de datos
- Notificación de vulnerabilidades — explotada activamente = incidente + conocimiento de explotación

Nota al margen: los productos que entran en el mercado también necesitan cumplir con los requisitos de salud y seguridad. La CRA no es clara en cuanto a cómo la evaluación de la conformidad de la ciberseguridad se relaciona con los requisitos de salud y seguridad (safety). El marcado CE solo se puede aplicar si se cumplen todos los requisitos para los productos.

NIS 2

NIS2 Art. 21 (2): Las entidades esenciales e importantes deben cumplir al menos:

- Realizar análisis de riesgos y contar con políticas de seguridad del sistema de información
- Tener procedimiento de manejo de incidentes (prevención, detección, respuesta)
- Continuidad del negocio: tales como — gestión de copias de seguridad, recuperación de desastres y gestión de crisis
- Seguridad de la cadena de suministro, incluidos los aspectos relacionados con la seguridad relativos a la relación entre cada entidad y los proveedores o proveedores de servicios = seguridad colectiva de la cadena ecológica **(véase también el artículo 22 NIS2)**
- Seguridad en sistemas de información de red relacionados con la adquisición, desarrollo y mantenimiento (incluido el manejo y divulgación de vulnerabilidades)
- Políticas y procedimientos: evaluar la eficacia de los procedimientos de gestión de riesgos de ciberseguridad
- Políticas y procedimientos para el uso de criptografía y cifrado
- Seguridad de RRHH, política de control de acceso y gestión de activos
- Uso de soluciones de autenticación multifactor/autenticación continua, comunicación segura de voz, vídeo y texto en sistemas de comunicación de emergencia seguros

NIS 2

Certificación de ciberseguridad: una herramienta para demostrar el cumplimiento Art. 24 NIS2

- La Comisión está facultada, mediante el acto delegado, para obligar a la certificación de ciberseguridad *de la UE a las categorías* de *entidades esenciales* e *importantes (artículo 24, apartado 2, NIS2) cuando se identifiquen niveles insuficientes de ciberseguridad*

- Antes de la elaboración de un acto delegado, se llevará a cabo una evaluación de impacto y «consultas» (presumiblemente, la realización de evaluaciones del sistema mediante consultas con las partes interesadas).

- Los Estados miembros tienen la oportunidad de exigir la certificación de ciberseguridad de la UE para las *entidades esenciales e importantes de determinados productos.*

- En caso necesario, la Comisión podrá solicitar un nuevo esquema de certificación (artículo 24, apartado 3, NIS2)

- Mediante Implementing Acts, la Comisión podrá especificar las especificaciones tecnológicas y metodológicas del artículo 21 NIS2: *esto puede tener un impacto en los productos certificados de la UE y en la adquisición de productos con elementos digitales.*

Chips Act

Pilares de la Ley de chips:

- **Iniciativa de chips para Europa**: desarrollo de capacidades tecnológicas a gran escala e innovación importante proyecto de interés común de la UE
- **Seguridad del suministro en crisis**: inversiones diseñadas y ejecutadas adecuadamente en la UE
- **Monitoreo y respuesta a crisis**: anticipar y regular la escasez

La junta semi conductora, entre otros, analizará:

«Necesidad de identificar **sectores y tecnologías específicos** con **un potencial de alto impacto social y la respectiva importancia de la seguridad** en la necesidad de **certificación** para productos confiables»

Comisión:

«La Comisión trabajará con los Estados miembros y el sector privado para determinar los requisitos sectoriales para los chips ‘trusted’ con vistas a establecer normas comunes y requisitos de certificación y contratación pública para aumentar la ciberresiliencia de las cadenas de suministro » (p. 4 Propuesta de Ley de Chips COM(2022) 46 final)

La relación con la CRA, NIS2, CSA, eIDAS2 y AI Act puede ser relevante.

EU Cyber Solidarity Act

Pilares:

- fortalecer la detección y la conciencia situacional de amenazas cibernéticas en toda la UE
- mejorar la preparación y las capacidades de respuesta
- fomentar la soberanía tecnológica europea en ciberseguridad

¿Cómo?

- red paneuropea de Centros de Operaciones de Seguridad (SOCs)
- establecimiento de un Mecanismo de Emergencia Cibernética y un Mecanismo Europeo de Revisión de Incidentes de Ciberseguridad
- mayor colaboración entre los estados miembros y con el sector privado
- financiación sostenida

Otros datos

- criterios para la selección de proveedores de confianza
- creación de una reserva de ciberseguridad de la UE,

Los SOCs usarán el esquema de certificación Managed Security Services.

European Digital Identity Regulation - Wallet

Pilares:

- A todos los ciudadanos de la UE se les ofrecerá la posibilidad de tener una Cartera de Identidad Digital de la UE para acceder a servicios en línea públicos y privados con total seguridad y protección de datos personales en toda Europa.
- Los servicios privados que están obligados legalmente a autenticar (instagram) a sus usuarios tendrán que aceptar el Wallet de la UE para iniciar sesión en sus servicios en línea.
- Además de almacenar de forma segura su identidad digital, el Wallet permitirá a los usuarios abrir cuentas bancarias, realizar pagos y conservar documentos digitales, como un permiso de conducir móvil, una receta médica, un certificado profesional o un billete de viaje.

Otros datos

- Nov 2023: acuerdo alcanzado por los colegisladores. Sujeto a la aprobación formal del Parlamento Europeo y del Consejo.
- Cuatro proyectos piloto a gran escala
- Aún no se han establecido las especificaciones técnicas

Alto grado de seguridad certificado de forma independiente y las partes relevantes de su código se publicarán en código abierto para excluir cualquier posibilidad de uso indebido, rastreo ilegal, rastreo o interceptación gubernamental..

AI Act

Pilares:

- Primera regulación integral en el mundo sobre el uso de la inteligencia artificial.
- Enfoque Basado en el Riesgo

¿Cómo?

- Se prohíben ciertos usos de la IA considerados una amenaza para las personas, como la manipulación cognitivo-conductual y el escaneo biométrico en tiempo real en espacios públicos, salvo en casos excepcionales

Otros datos

- excluye de su aplicación a los sistemas de IA utilizados con fines de seguridad nacional, defensa y militares, así como aquellos utilizados únicamente con fines de investigación y desarrollo

Sistemas de IA en áreas críticas como la gestión de infraestructuras esenciales, educación, empleo, servicios públicos y privados esenciales, aplicación de la ley, entre otros, deberán ser evaluados antes de su lanzamiento al mercado y a lo largo de su ciclo de vida .

CONTENIDO

Conclusiones

Riesgos

- **Recursos:** Implementación **desigual** entre los Estados Miembros.
- **Complejidad: Dificultades en el cumplimiento** por parte de entidades privadas y públicas.
- La legislación puede quedarse rápidamente **obsoleta** frente a la rápida evolución tecnológica.
- **Interpretaciones:** Riesgo de **fragmentación del mercado** digital de la UE.
- **Recursos** insuficientes para **monitoring** adecuado..

Oportunidades

- Mejora en la **protección** contra ciberamenazas y en la gestión de incidentes.
- Aumento de la **confianza** en el mercado digital a través de la certificación de ciberseguridad.
- Fomento de la **innovación** y la competitividad de las empresas europeas.
- Potencial de la legislación europea para convertirse en un **referente global** en ciberseguridad.
- Refuerzo de la **resiliencia** económica y la seguridad colectiva de la UE.


jtsec
BEYOND IT SECURITY
Gracias

CRA y CSA

Incumplimiento

Certificación de ciberseguridad de la UE con arreglo a la CRA y el incumplimiento: algunos ejemplos:

- CRA: El organismo notificador designado por el Estado miembro (libre elección, puede ser el NAB o cualquier otro organismo) está facultado para suspender o retirar el certificado de un fabricante cuando compruebe que hay un incumplimiento. (artículo 37, apartado 5, de la CRA) ¿Qué sucede si un Estado miembro opta por designar a un organismo distinto del NAB como organismo notificador en virtud de la CRA y existe una presunción de conformidad para la certificación de ciberseguridad (siendo el NAB el único organismo que acredita)? ¿Ambos organismos notificantes supervisan el CAB? ¿Debería haber una doble notificación bajo CSA y CRA?
- CRA: El organismo notificado (CAB) está facultado para suspender o retirar el certificado de un fabricante cuando compruebe que hay un incumplimiento. (artículo 37, apartado 5, de la CRA) ¿Por qué la restricción del certificado de evaluación no es legalmente posible en esta situación? Puede ser útil tener la oportunidad de restringir temporalmente un certificado hasta que se hayan tomado medidas correctoras. ¿Qué sucede si bajo CSA se restringe un certificado y el certificado se expide bajo una presunción de conformidad con la CRA, quién está evaluando las consecuencias de la CRA?
- El antiguo artículo 18, apartado 4, de la CRA: presunción de conformidad y especificación del certificado de ciberseguridad de la UE que elimina la obligación de realizar una evaluación de terceros: necesidad de especificar las normas relativas a la supervisión y la supervisión (CSA: NAB & NCCA en relación con la CRA: función de la Comisión ex art. 36 CRA en los CAB no conformes, = necesidad de informar a la autoridad de vigilancia del mercado en caso de incumplimiento de los certificados no conformes debido a un CAB no conforme. ¿Cómo pueden utilizarse las competencias conexas de la NCCA y la Comisión por quién y la coordinación necesaria entre las diferentes autoridades y organismos teniendo en cuenta que también pueden aplicarse otros Reglamentos (por ejemplo, NIS2, eIDAS2, AI Act y, posiblemente, la Ley de Chips) para garantizar un enfoque armonizado y coherente?

CRA y CSA

Incumplimiento

Otro ejemplo: Certificación de ciberseguridad de la UE con arreglo a la CRA e incumplimiento:

- **Producto certificado CSA que no cumple con la CRA:** La Comisión está facultada para *derogar o modificar* una *presunción de certificación de ciberseguridad de la UE*l si el incumplimiento del producto se atribuye a deficiencias del esquema *(control de cumplimiento ex post) (artículo 44, apartado 4, de la CRA) ¿Debería/puede 1 producto incumplidor dar lugar a la derogación de la presunción de certificación IA?*

- ***Consecuencias:*** *la no conformidad de un producto puede dar lugar a la derogación o modificación de una «supresión» completa de la presunción de conformidad de un régimen. Parece más probable que el suplemento CRA pueda necesitar una «revisión» en consonancia con el artículo 48 de la CSA. Los certificados podrían suspenderse o restringirse mientras tanto, si se considera necesario. La derogación de la presunción de conformidad IA, de hecho, haría inútil la certificación con arreglo al régimen aplicable, ya que todos los productos certificados ya no cumplen los requisitos de CRA, bloqueando cualquier acceso al mercado de la UE.*

- Si la Comisión deroga la evaluación de impacto, todos los productos certificados tendrían que ser reevaluados

- ¿Mientras tanto no hay acceso al mercado?

- ¿Qué sucede con los productos en el mercado?

- ¿Reclamaciones de responsabilidad por «pérdida» de valor de los certificados?

- En estas circunstancias, ¿quién está tomando qué tipo de acciones?

La decisión de derogar debe incluir al menos medidas transitorias y proporcionar seguridad jurídica a los agentes del mercado y garantizar que se tengan en cuenta los principios de competencia leal.

CRA y CSA

Incumplimiento

Certificación de ciberseguridad de la UE en virtud de la CRA y (no)cumplimiento:

- Artículo 41, apartado 3, de la CRA: Las autoridades de vigilancia del mercado cooperarán con las NCCA e intercambiarán información periódicamente.
  - Recomendación: individual y colectivo: ECCG y ADCO — representantes de las autoridades de vigilancia del mercado y de las oficinas únicas de enlace)

- Papel de apoyo deENISA en el incumplimiento de productoscon riesgos significativos de ciberseguridad (artículo 45 de la CRA):
  - proporcionar información (basada en incidentes y vulnerabilidades conocidas) a la Comisión
  - situaciones excepcionales a escala de la Unión: La Comisión podrá pedir a ENISA que facilite una evaluación de la conformidad y tome, previa evaluación y consulta a los Estados miembros y a los agentes económicos a escala de la Unión, una medida restrictiva (retirada/recordación del producto del mercado)

- Producto conforme pero con riesgos significativos de ciberseguridad (tras la información a ENISA): retirar del mercado el producto (artículo 46 de la CRA)
  - Riesgo para la salud y la seguridad (safety), cumplimiento de la legislación de la UE o nacional, derechos fundamentales o autenticidad/confidencialidad/integridad de los servicios, o utilizado en sistemas de información por entidades esenciales según la NIS2 (anexo I NIS2) -> TBD: considerar la obligación de utilizar la certificación de la UE en el nivel de garantía adecuado

Otras regulaciones: CRA

Relaciones con la otra ley de la UE

Certificación de ciberseguridad: incumplimiento del artículo 21 de la NIS2

- Si no se cumplen los plazos impuestos por la Autoridad NIS2, los Estados miembros garantizarán con respecto a las entidades esenciales:
  - ¿La autoridad competente de NIS2 2 está facultada para *suspender temporalmente o solicitar una certificación temporal* al organismo de autorización? O bien solicitarlo directamente al OC, solicitarlo directamente al OC (artículo 32, apartado 5 bis, NIS2).

- Nota al margen: entidades importantes no incluidas en la posibilidad de suspensión temporal de la certificación: ¿el certificado permanece intacto o dejado en manos de la NCCA?

- En el marco del CRA: el producto será retirado o retirado del mercado (Art: 47 (1-2) CRA

- En el marco de la CSA: el certificado se retirará si el organismo de certificación no cumple las medidas atenuantes en el plazo previsto (disposición propuesta en el Reglamento de Ejecución).

- En virtud de la Ley de IA: Si el incumplimiento persiste después de haber sido instruido para poner fin al incumplimiento por parte de la Autoridad de Vigilancia del Mercado y no se han seguido instrucciones, la IA se retirará de la Ley de IA del artículo 68 (1-2) del mercado.

Otras regulaciones

Estudios de viabilidad de certificación de ciberseguridad

Certificación de ciberseguridad vs. CRA, AI Act, eIDAS & NIS2:

- Mapeo de los requisitos de ciberseguridad de las diferentes legislaciones de la UE a la CSA;
- Estudio sobre lo que puede ser cubierto por qué esquema (elementos)?
- ¿Cuánto tiempo se aplican los requisitos (enfoque del ciclo de vida)?
- ¿Obligaciones de manejo de vulnerabilidades e informes de incidentes? Los diferentes procedimientos de presentación de informes a los diferentes organismos con plazos diferentes pueden requerir una cuidadosa consideración para garantizar la eficacia y eficiencia de la presentación de informes.
- B) Gobernanza: Notificaciones, funciones y responsabilidades y colaboración: mecanismos de coordinación entre los diferentes organismos de supervisión y supervisión (¿sistema de autoridad principal?)
- ¿Qué hacer cuando en la tramitación de reclamaciones y en los procedimientos de incumplimiento y ejecución, las leyes de la UE se tocan entre sí? (Aplicación/acto delegado? Podría resolver el asunto)
- Son necesarias normas claras sobre la aplicación del marcado CE en relación con las marcas y etiquetas utilizadas en el marco de la certificación de ciberseguridad
- Aplicar y coordinar múltiples sistemas de penalización: multas emitidas por diferentes autoridades y siguen siendo efectivas, proporcionadas y disuasorias

CRA

Relaciones con el otro derecho de la UE

Directiva NIS2: Las entidades esenciales e importantes deben: (Art. 21 NIS2)

- Tomar medidas técnicas y de organización (TOMs)
- Adecuado al nivel de riesgo presentado para minimizar el impacto de los incidentes en los destinatarios y otros servicios (= seguridad de la cadena de suministro superior + recomendación: incluir en las medidas seguridad de la cadena de suministro ascendente = entregar productos y servicios seguros a entidades esenciales e importantes)
- Visto el estado de la técnica
- Proporcionalidad de las TOM:
  - grado de exposición a riesgos;
  - el tamaño de la entidad,
  - probabilidad de ocurrencia de incidentes y su gravedad — impacto social y económico
- Proteger la red y los sistemas de información y el entorno físico de los incidentes

CRA

Relaciones con el otro derecho de la UE

Sistemas de IA bajo la CRA y certificados bajo CSA: consecuencias

Los sistemas de IA de alto riesgo (sin perjuicio de los requisitos de precisión y robustez) **deben cumplir:**

- Requisitos esenciales CRA (sección 1 y 2 anexo 1)
- Requisitos de ciberseguridad en virtud del artículo 15 de la Ley de IA
- Requisitos de la CSA Art. 51 CSA

- **Los CABs deben cumplir con la norma indicada y:**
  - CRA: Artículo 29 Requisitos de los CAB — Comisión para comprobar el incumplimiento/denuncias — artículo 36 de la CRA
  - Ley de IA: Artículo 33 Requisitos de los CAB — Comisión de control de las denuncias/incumplimiento (artículo 37 de la Ley de IA)
  - CSA: Anexo 1 requisitos y, en su caso, requisitos de autorización — NAB & NCCA para el incumplimiento y disposición legal para reclamaciones

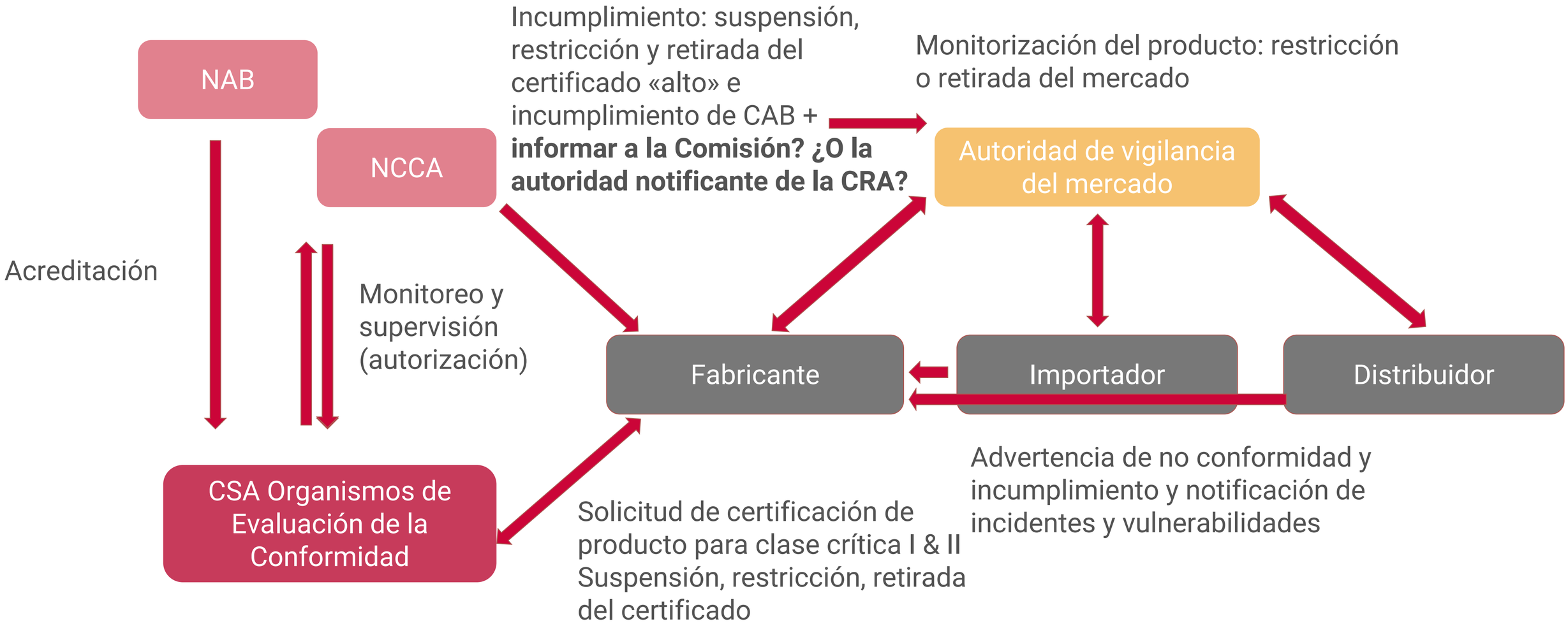
CRA

Gobernanza CRA vs CSA

¿Informar del incumplimiento del papel del CAB?

CRA

Gobernanza CRA vs CSA



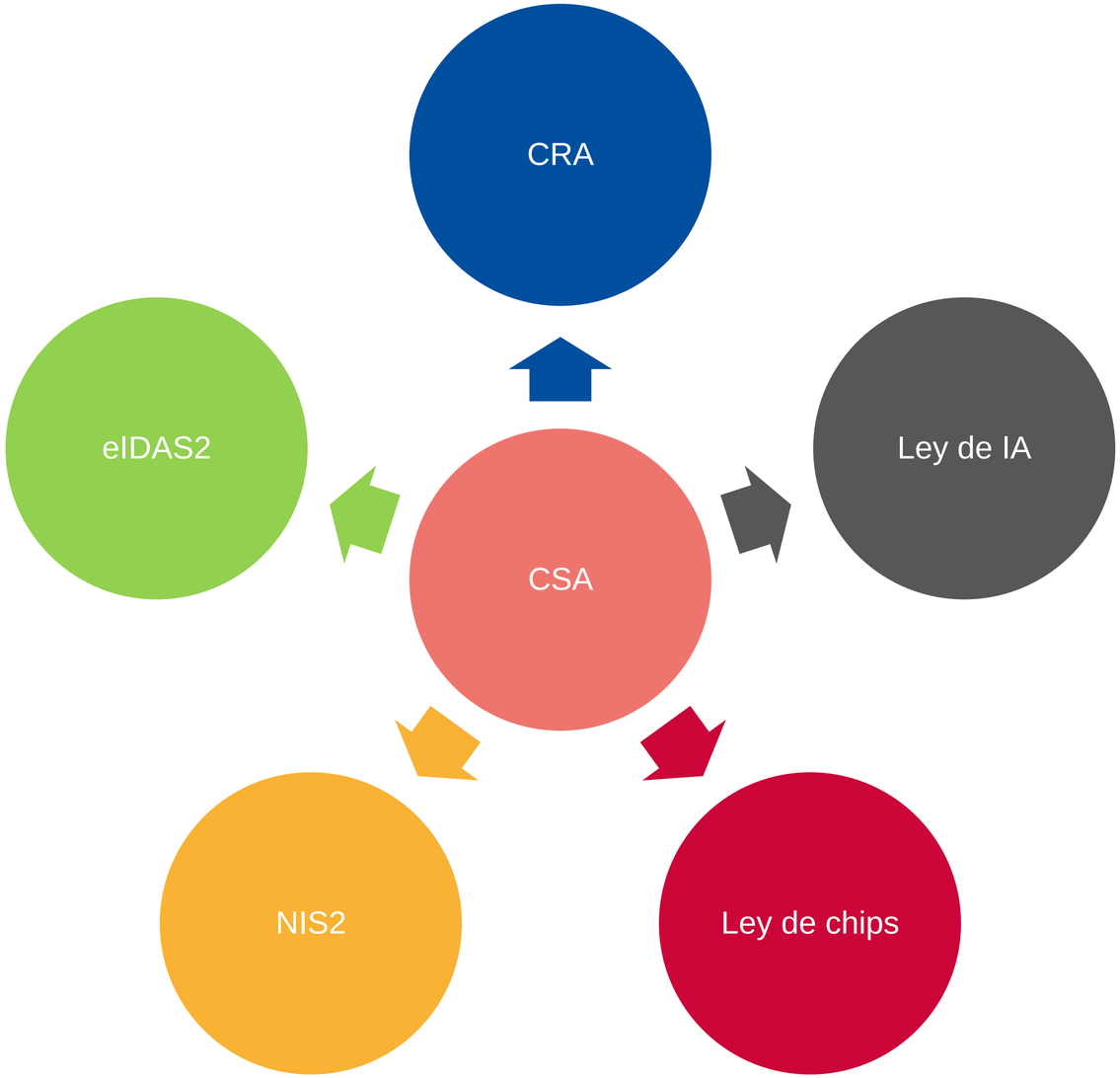
Auditoría vs Cumplimiento legal

¿Qué diferencia hay entre auditoría y cumplimiento legal?

- Si te pillan te multan
- ¿Dónde aplica en España?
  - RGPD: De conformidad a los artículos 24 y 32 del Reglamento Europeo de Protección de datos (RGPD), el responsable del tratamiento, en este caso la empresa o la organización, tiene la obligación de garantizar la seguridad de los datos de carácter personal que haya recabado.
  - Ley PIC: Necesidades de protección de infraestructuras críticas
  - Directiva NIS: Como Ley PIC pero a nivel Europa.
  - ENS: Sistemas certificados para las AAPP y sus proveedores.

Puntos de vista estratégicos
Sobre el desarrollo de esquemas

Certificación de ciberseguridad referida
en las diferentes leyes de la UE



CRA

Cómo cumplir con los requisitos esenciales

Presunción: Es necesario mapear los requisitos de CSA y CRA — ¿Por qué?

Consecuencias:

- Un esquema de ciberseguridad de la UE que no se ajuste plenamente a los requisitos de CRA requeriría que el fabricante se sometiera **además a una evaluación por la CRA de los elementos no cubiertos** para poder entrar en el mercado
- → Los esquemas de la UE que certifiquen productos, servicios o procesos de TIC que se encuentren dentro del ámbito de aplicación de la CRA deben cumplir los requisitos de la CRA
- Crear un mapeo planificación sobre cómo llenar los vacíos identificados: desarrollar un **«suplemento CRA»** al conjunto de requisitos que deben añadirse e incluirse en la certificación, pero: ¿con alcance de un máximo de 5 años?
- **¿Qué sucede después de 5 años** con los productos que cumplen con CRA pero tienen un ciclo de vida más largo o una «segunda vida»? ¿Ya no es necesario cumplir con los requisitos e informar de las vulnerabilidades e incidentes? La certificación de ciberseguridad garantiza mantener la seguridad cibernética: el nivel de garantía se corresponde con los riesgos en evolución a lo largo del tiempo hasta el final de la vida útil.

CRA

NIS2 y notificación de vulnerabilidades

La presentación de informes (artículo 11) en el plazo de 24 horas apunta claramente a NIS2:

- Vulnerabilidades explotadas activamente notificadas a ENISA que hará forward al CSIRT para coordinar la divulgación de vulnerabilidades e informar a la autoridad de vigilancia del mercado
- Los incidentes con impacto en la ciberseguridad de los productos con elementos digitales notifican a ENISA que hará forward a los puntos de contacto únicos de los Estados miembros, en caso necesario, a CyCLONe (incidentes transfronterizos a gran escala)
- Responsabilidad de ENISA: preparar un informe técnico bienal sobre las tendencias emergentes de los riesgos de ciberseguridad y el panorama de amenazas.

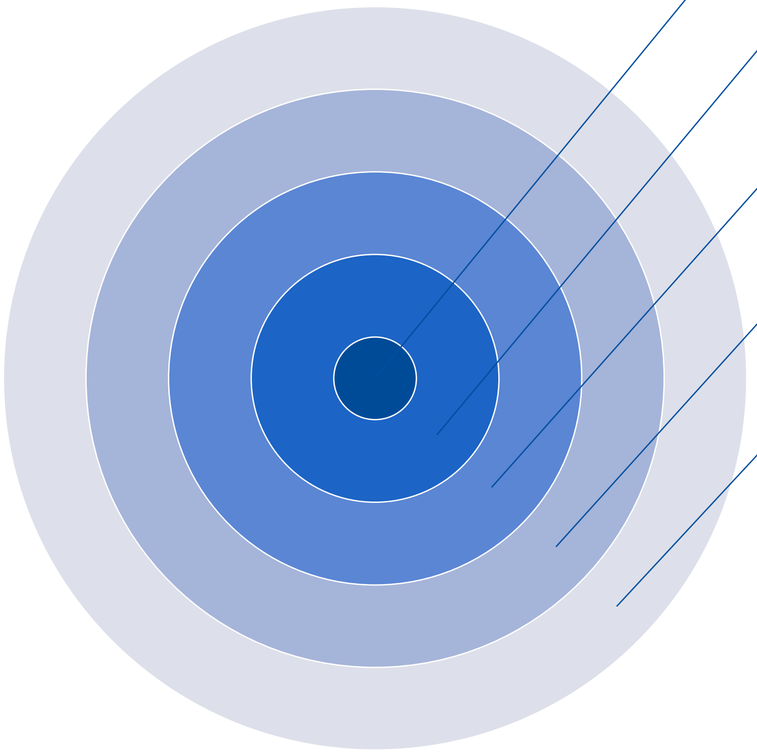
CRA

Ley de IA bajo la CRA

- La **Ley de IA utiliza los mismos 3 enfoques** para la presunción de conformidad (artículo 42 de la Ley de IA) para cumplir con las normas armonizadas/requisitos de evaluación de AI y CRA y ajustar los requisitos de evaluación de la certificación de ciberseguridad
- **Los sistemas de IA de alto riesgo deben cumplir los requisitos esenciales** (sección 1 y 2), estos requisitos también cumplen los requisitos de ciberseguridad establecidos en el artículo 15 de la Ley de IA, sin perjuicio de los requisitos de exactitud y solidez
- **Se aplica el procedimiento de evaluación de la conformidad del** artículo 43 de **la Ley de IA**
- **Declaración de conformidad** o en el caso de **evaluación de tercera parte, un certificado de evaluación**
- Debe aplicarse **Marcado CE** antes de entrar en el mercado de la UE
- **Las CAB notificadas** en virtud de la Ley de IA también pueden **evaluar la conformidad de acuerdo al CRA**, siempre que cumplan los requisitos para CABs del artículo 29 de la CRA
- **PERO si la IA se utiliza en las clases críticas I y II**: una **evaluación de tercera parte bajo CRA** aplica para los requisitos esenciales
- Producto de inteligencia artificial clasificado altamente crítico: Art 6 (5) CRA — La Comisión puede obligar a la Certificación de Ciberseguridad

CRA

Relaciones con el otro derecho de la UE



Productos, servicios y procesos de TIC (requisitos de contratación pública)

Reglamentos específico o sectoriales (e.g., la Ley de Chips)

Directiva NIS 2

Ley de IA

Ley de ciberresiliencia

Certificación de ciberseguridad sirviendo como presunción de conformidad

NIS 2

Responsabilidad de tercer nivel

(1) Los Estados miembros garantizan que 2) toda persona física:

- Actuando como representante o con **poder para representarlo**
- **Tiene autoridad** para tomar **decisiones**
- Tiene autoridad para **ejercer el control**

Los Estados miembros velarán por que las autoridades competentes dispongan de:

- la facultad de imponer una prohibición temporal contra cualquier persona que ejerza responsabilidades de dirección a nivel de CEO o representante legal, o contra una persona física considerada responsable de la violación del ejercicio de funciones directivas.

- ✓ Tiene competencias para garantizar su cumplimiento
- ✓ Puede ser considerada responsable del incumplimiento de sus obligaciones (como entidad esencial o importante) en virtud de NIS2
- ✓ *La certificación reduce la responsabilidad*