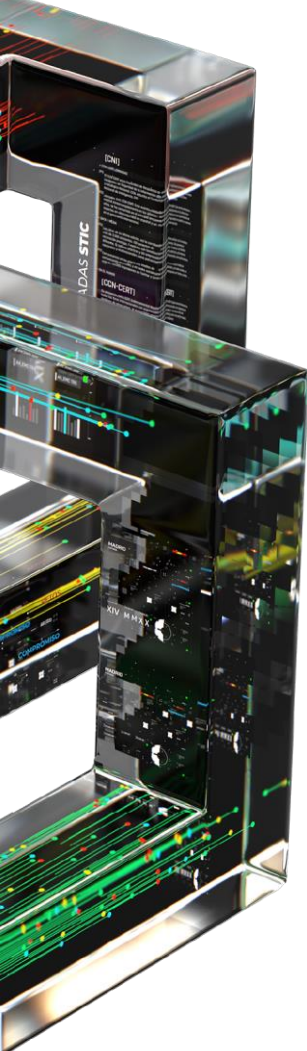




#XIVJORNADASCCNCERT

**“La certificación de
ciberseguridad en Europa,
un desafío común”**



Javier Tallón Guerri

jtsec: Beyond IT Security

jtallon@jtsec.es

- ❑ Ingeniero en Informática (Universidad de Granada)
- ❑ Co-Fundador & Director Técnico en **jtsec Beyond IT Security S.L.**
- ❑ Full-stack ~~hacker~~ wannabe
- ❑ Experto en Common Criteria, Lince, PCI-PTS, FIPS 140-2, ISO 27K1, SOC2
- ❑ Profesor del Máster de Ciberseguridad en la Universidad de Granada
- ❑ 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

La certificación de ciberseguridad en Europa, un desafío común



Antecedentes

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.



Centro Nacional de Inteligencia

2002



Organismo de Certificación

2007

Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información

Centro Criptológico Nacional



2004

Se asigna al CCN la responsabilidad de la certificación de la ciberseguridad.

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



LINCE

2018

Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad

SOG-IS

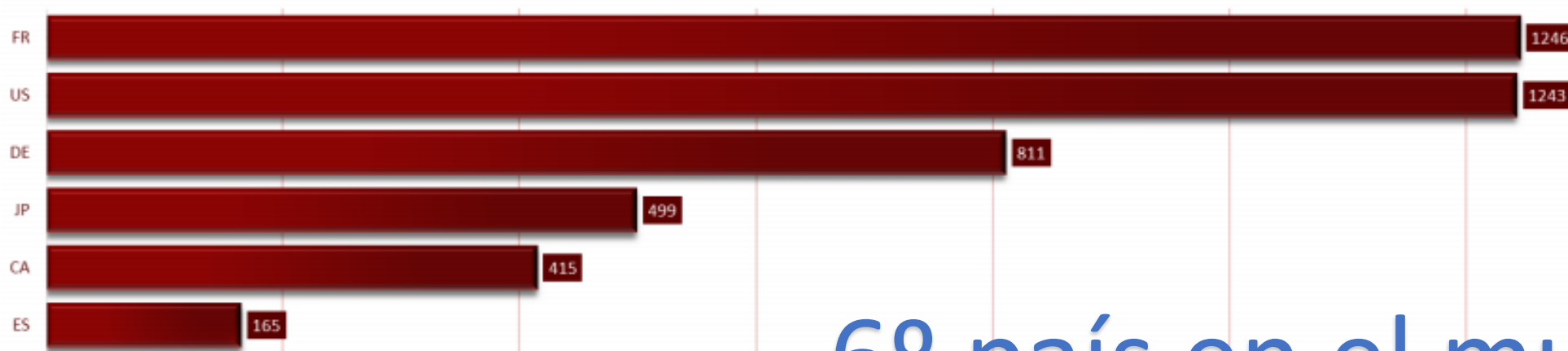
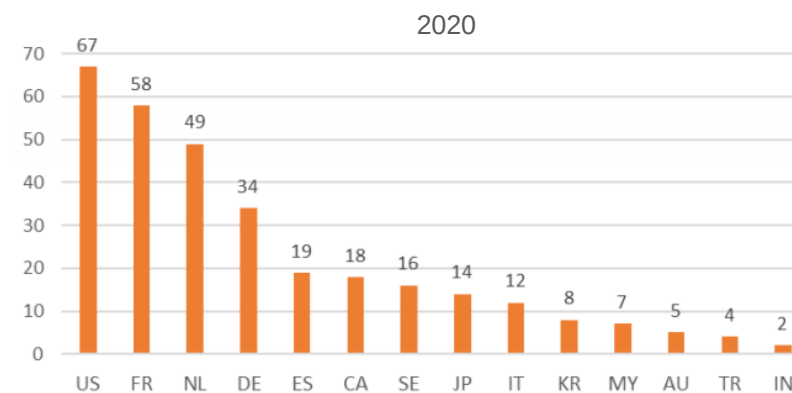
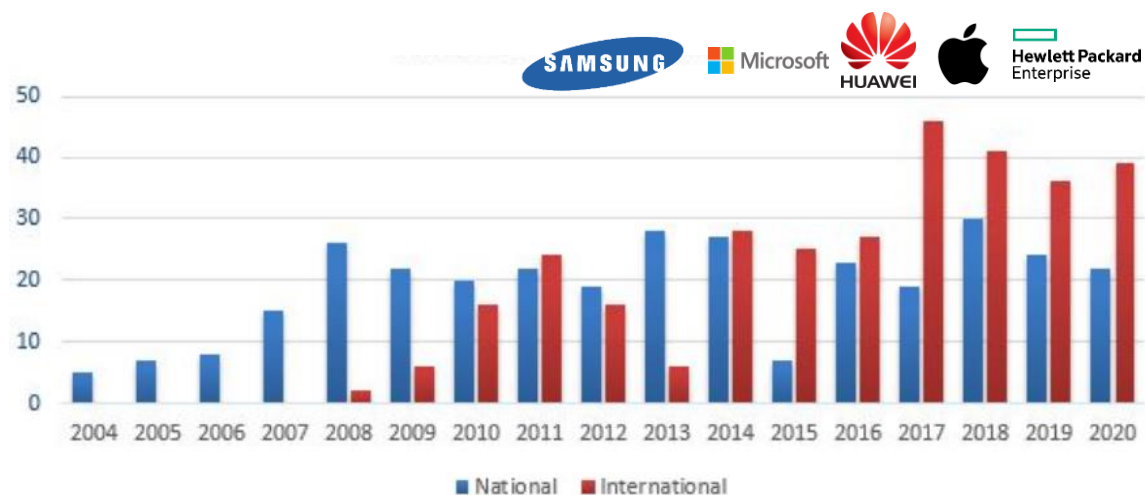
2010

Senior Officials Group Information Systems Security



La certificación de ciberseguridad en Europa, un desafío común

Antecedentes



6º país en el mundo

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.

La certificación de ciberseguridad en Europa, un desafío común

Antecedentes



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.



La certificación de ciberseguridad en Europa, un desafío común

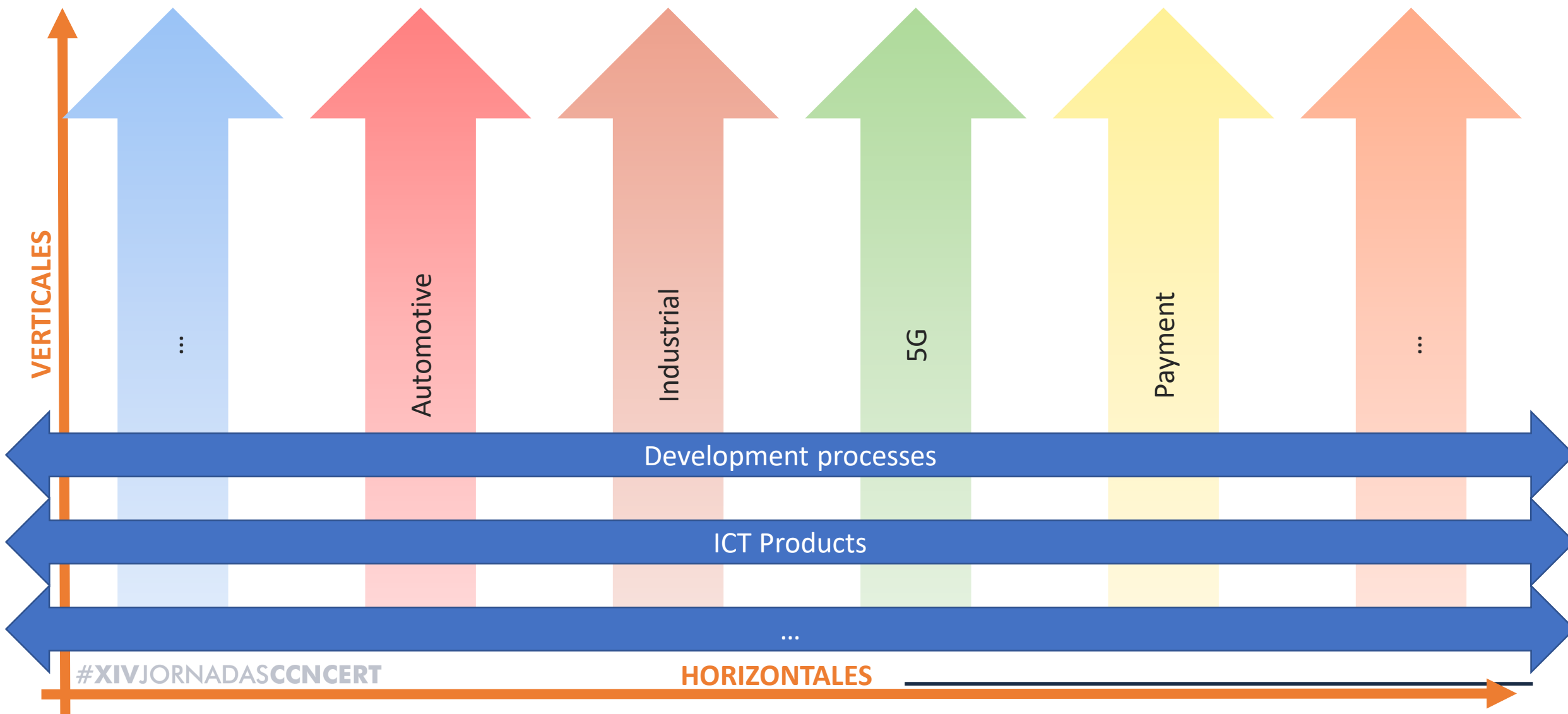
Antecedentes



- 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

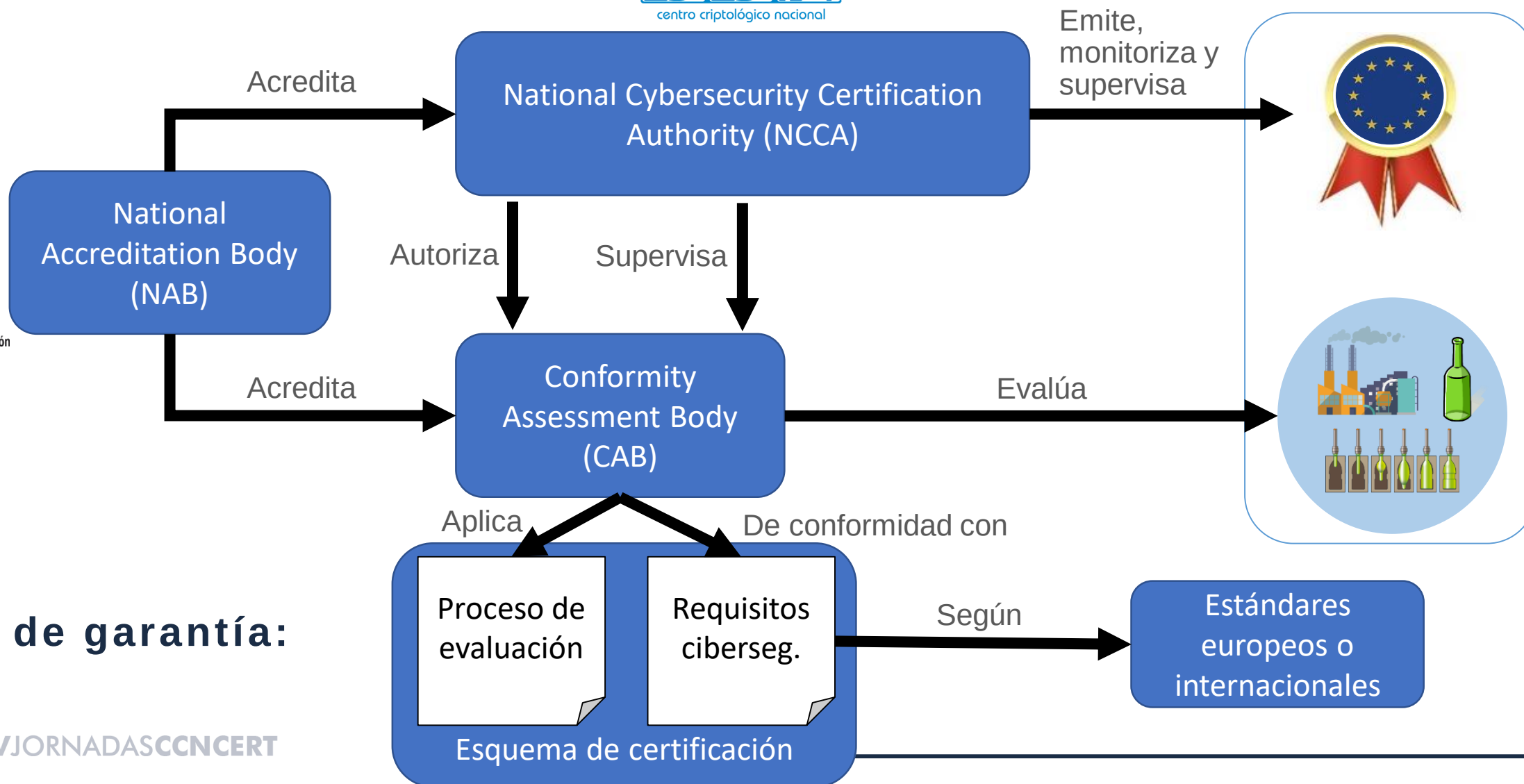
La certificación de ciberseguridad en Europa, un desafío común

Antecedentes



La certificación de ciberseguridad en Europa, un desafío común

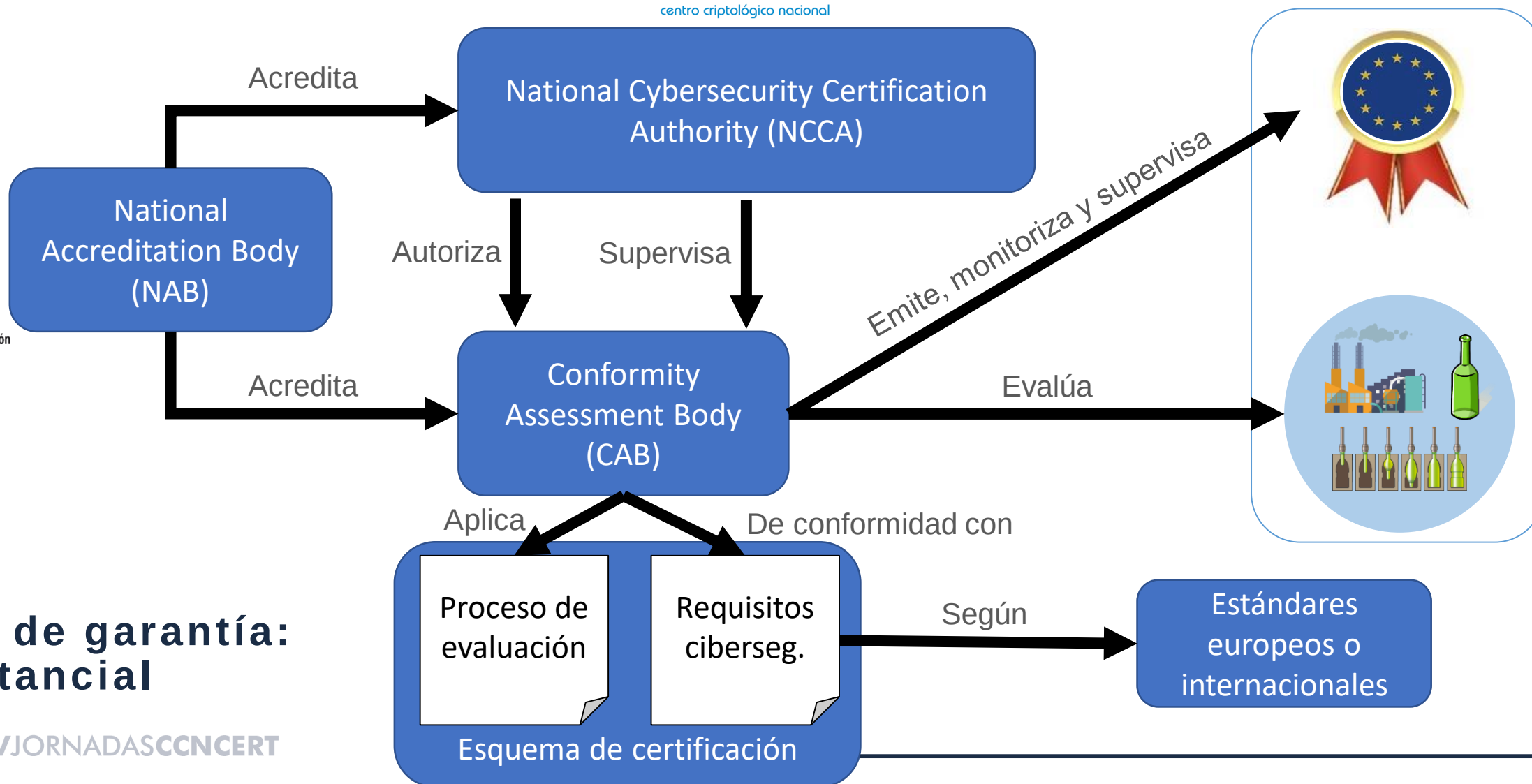
Antecedentes



**Nivel de garantía:
Alto**

La certificación de ciberseguridad en Europa, un desafío común

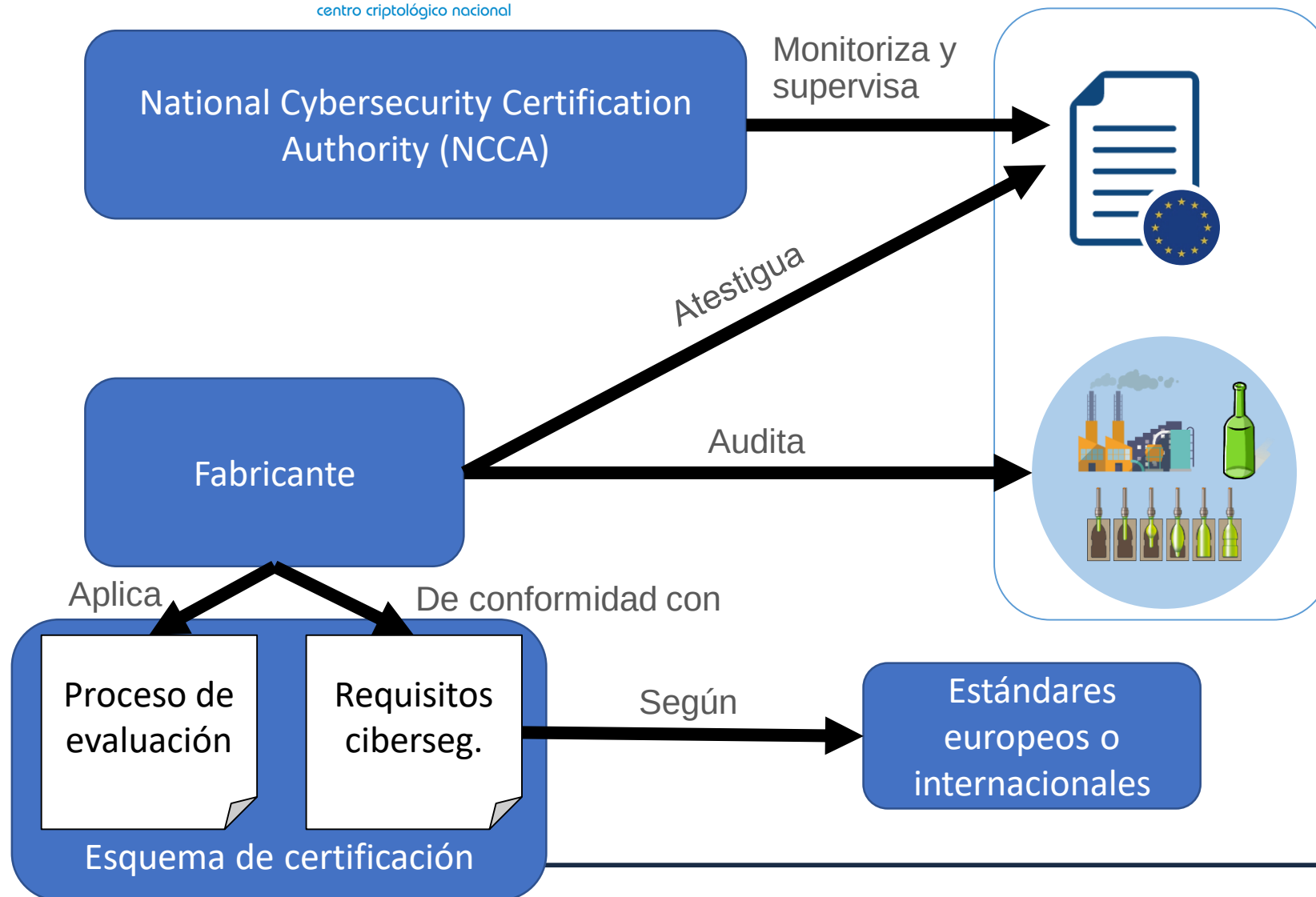
Antecedentes



**Nivel de garantía:
Substancial**

La certificación de ciberseguridad en Europa, un desafío común

Antecedentes



**Nivel de garantía:
Básico**

La certificación de ciberseguridad en Europa, un desafío común

Antecedentes

Nivel	¿Qué se prueba?	Objetivo	Tipo de evaluación mínima	¿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

La certificación de ciberseguridad en Europa, un desafío común

Antecedentes

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

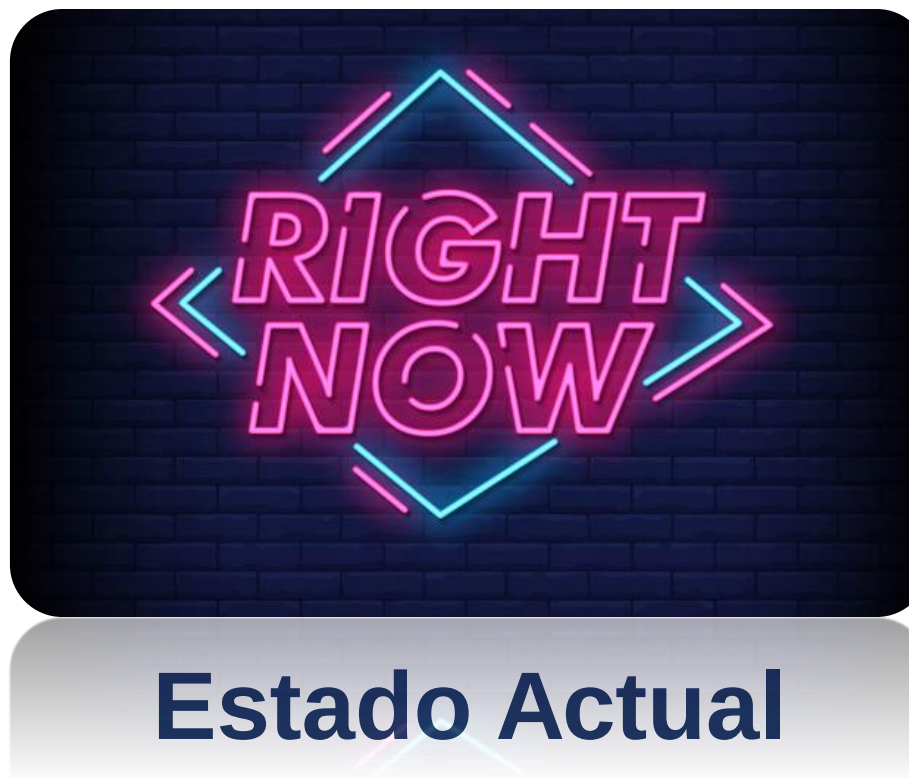
- Análisis del panorama de amenazas
- Potencialmente repetir evaluaciones

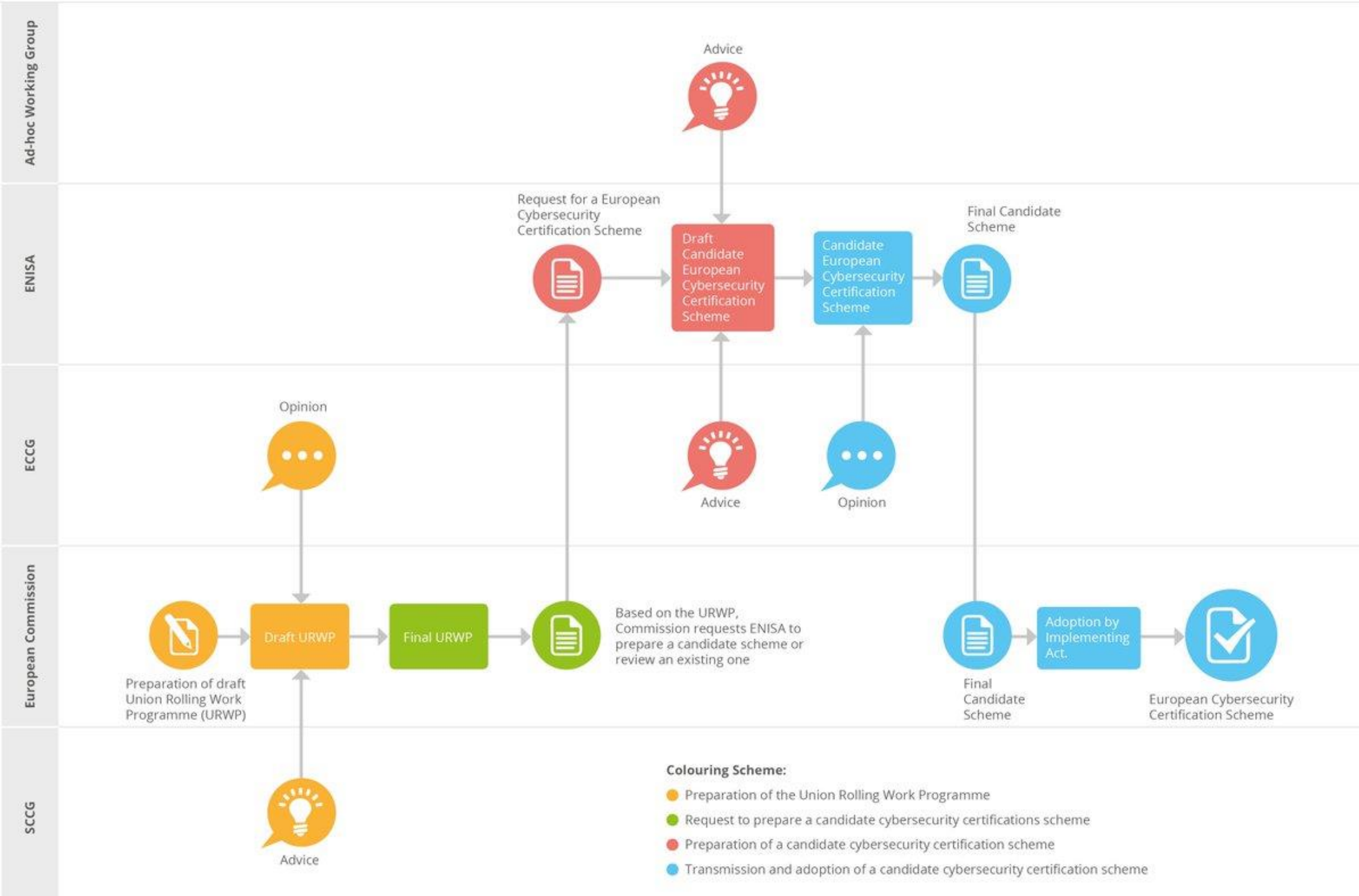
La certificación sigue siendo voluntaria... hasta que se indique lo contrario.

- Prevista revisión por la Comisión Europea en 2023



La certificación de ciberseguridad en Europa, un desafío común





La certificación de ciberseguridad en Europa, un desafío común

Estado actual

- EUCC
 - Esquema de certificación de **productos** para niveles substancial y alto
 - Trasposición del **SOG-IS**: Good old Common Criteria
 - Primera versión ya sometida a consulta pública
 - Al Adhoc Working Group sigue activo para resolver
 - **Q2 2021 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



La certificación de ciberseguridad en Europa, un desafío común

Estado actual

- **Servicios Cloud**
 - Esquema de certificación de servicios para niveles básico, substancial y alto
 - No self-assessment
 - Se lanza Adhoc WG en Marzo de 2020
 - Parte del trabajo de **CSPCert**
 - Usa el lenguaje de ISO/IEC 17788 (Infraestructura / plataforma / aplicación)
 - Metodología similar a ISO270xx / ISAE. Controles similares a los de C5 del BSI.
 - Considera el uso de “Complementary User Entity Controls”
 - Se espera **primera versión del esquema candidato para final de año**
 - **Afectará a todos los proveedores de servicios cloud**



La certificación de ciberseguridad en Europa, un desafío común



Futuro

La certificación de ciberseguridad en Europa, un desafío común

Futuro

- **Prioridades estratégicas**
 - Estandarización
 - Seguridad por diseño, seguridad del ciclo de vida y seguridad por defecto
 - Garantía basada en riesgos
 - Coherencia, “componibilidad”
 - Cooperación internacional

URNP



La certificación de ciberseguridad en Europa, un desafío común

Futuro

URNP

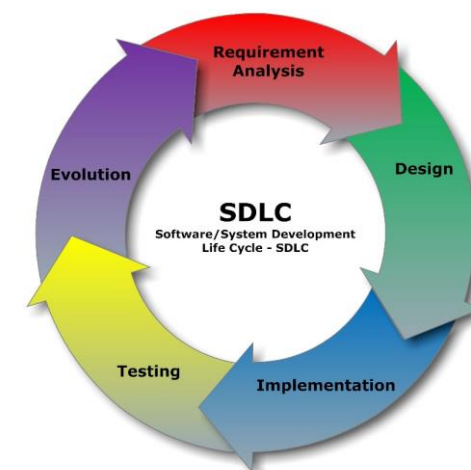
- **Nuevos esquemas**
 - Componentes Industriales (IACS)
 - Los sistemas de control industrial son construidos como la integración de múltiples y dispares componentes hardware/software
 - Asegurar IACS asegurando sus componentes
 - Hay una propuesta de ERNCIP (European Reference Network for Critical 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
 - Servicios críticos dependerán del 5G
 - Contemplado desde la publicación de la EU Toolbox
 - Potenciales metodologías: GSMA NESAS, Common Criteria



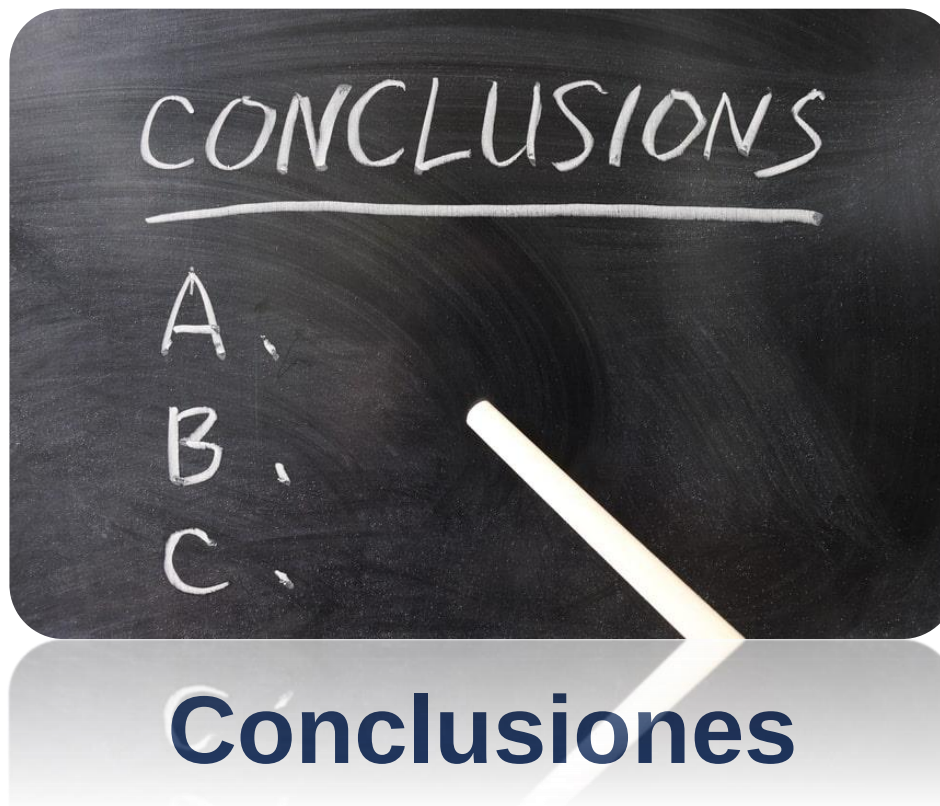
La certificación de ciberseguridad en Europa, un desafío común

Futuro

- Potenciales nuevos esquemas



La certificación de ciberseguridad en Europa, un desafío común



La certificación de ciberseguridad en Europa, un desafío común

Conclusiones

- Ciudadanos
 - Gracias al CSA la mejora en la ciberseguridad para todos será evidente
 - El ciudadano está en el centro de las políticas europeas de ciberseguridad. Europa lo hace por ti.



La certificación de ciberseguridad en Europa, un desafío común

Conclusiones

- **Fabricantes / Proveedores**
 - Momento de oportunidad para mejorar la competitividad con respecto a las empresas extranjeras
 - Hay que ponerse las pilas y estar preparados
 - Riesgo! Nuevos players europeos



La certificación de ciberseguridad en Europa, un desafío común

Conclusiones

- Administración española
 - Responsabilidades de la NCCA:
 - Controlar la conformidad de todos los certificados
 - Controlar el cumplimiento de las obligaciones de fabricantes y proveedores
 - Apoyar a las entidades de acreditación
 - Autorizar y auditar a los CABs
 - Tramitar las reclamaciones a los certificados
 - Imponer sanciones
 - Cooperar con otras NCCAs intercambiando información
 - Estar al día del panorama de la ciberseguridad
 - Sin inversión gubernamental YA para dotar a la NCCA de los recursos necesarios la posibilidad de que perdamos el tren de la competitividad es REAL



La certificación de ciberseguridad en Europa, un desafío común

Conclusiones

CSA, Artículo 58.5 “*Los Estados miembros velarán por que las autoridades nacionales de certificación de la ciberseguridad dispongan de los **recursos adecuados** para ejercer sus competencias y llevar a cabo, de manera eficaz y eficiente, las tareas que tienen encomendadas.*”

La certificación de ciberseguridad en Europa, un desafío común

Contacto

jtsec: Beyond IT Security

Granada & Madrid

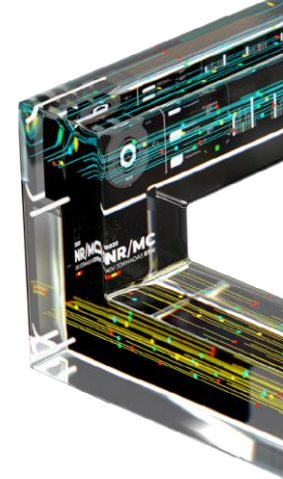
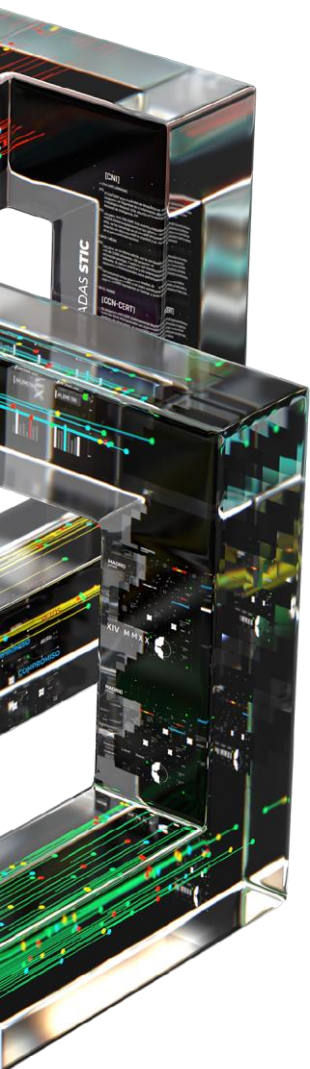
hola@jtsec.es

@jtsecES

www.jtsec.es



“Cualquier loco puede realizar algo complicado. Se necesita un genio para hacerlo simple.”
Woody Guthrie



MUCHAS GRACIAS

#XIVJORNADASCCNCERT