jtsec

BEYOND IT SECURITY

jtsec
BEYOND IT SECURITY

jtsec
BEYOND IT SECURITY

PTS | PARQUE TECNOLÓGICO DE LA SALUD

¿Quién soy?

- **Javier Tallón – @javiertallon**
- More than 12 years working in IT Security
- Full-stack ~~hacker~~ wannabe
- Certification Expert, member of the ENISA EUCC AhWG
- Cyber Security Teacher at UGR
- Certified Information Systems Security Professional
- Offensive Security Certified Professional

jtsec
BEYOND IT SECURITY

- **jtsec Beyond IT Security - @jtsecES**
- Services
  - CCN Accredited lab for LINCE & CC
  - Certification & cybersecurity consultancy
  - Ethical hacking
- Created in July'17 ~ 12 Employees
- Based in Spain (Granada and Madrid)

Índice

- El apasionante mundo de la auditoría de ciberseguridad
- Auditoría vs Certificación
- El framework europeo de certificación y los nuevos esquemas
- El panorama regulatorio de la cibersalud

El apasionante mundo de la auditoría de ciberseguridad

El apasionante mundo de la auditoría de ciberseguridad

El apasionante mundo de la auditoría de ciberseguridad

El apasionante mundo de la auditoría de ciberseguridad

El apasionante mundo de la auditoría 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 auditoría 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 auditoría 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 auditoría de ciberseguridad

- ¿Por qué auditar?
  - Independencia crítica
  - Es mejor auditarte tu mismo antes de que un ciberdelincuente te audite.

El apasionante mundo de la auditoría de ciberseguridad

- ¿Qué clase de pruebas puedo esperar en mi sistema?

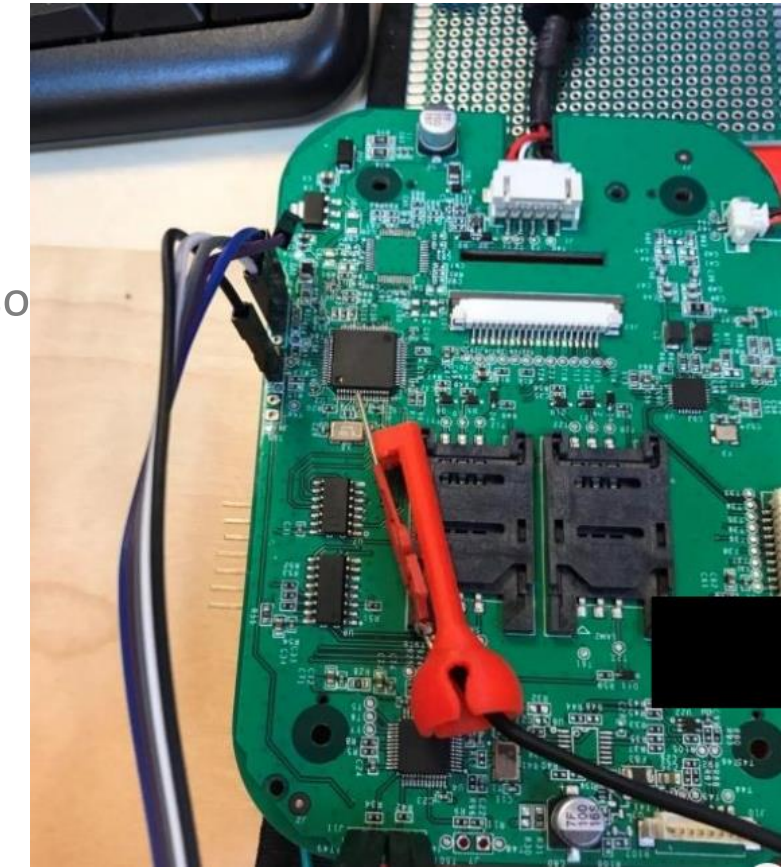
  - Técnicas
    - Ataques a las redes wifi
    - Rogue Aps
    - Ataques al directorio activo
    - Ataques de fuerza bruta / diccionario
    - Uso de keyloggers
    - USB Dropping
    - Ataques de phishing/vishing/ingeniería social
    - Búsqueda de vulnerabilidades públicas
      - Explotación de las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

El apasionante mundo de la auditoría 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 auditoría 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 auditoría de ciberseguridad

- ¿Qué clase de pruebas puedo esperar en mi producto?
  - No técnicas
    - Documento el ciclo de vida y la gestión de las claves
    - Uso de metodologías de desarrollo seguro
    - 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
    - Sitio de desarrollo seguro

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.

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

- **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

Applus+

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. (e.g. PCI)
  - Organizaciones internacionales cuyo único fin es precisamente escribir normas. (e.g. ISO, UNE, ETSI, CEN/CENELEC, …)
  - Administraciones públicas o estados (e.g. CCN, ENISA)

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 producto o sistema 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**

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

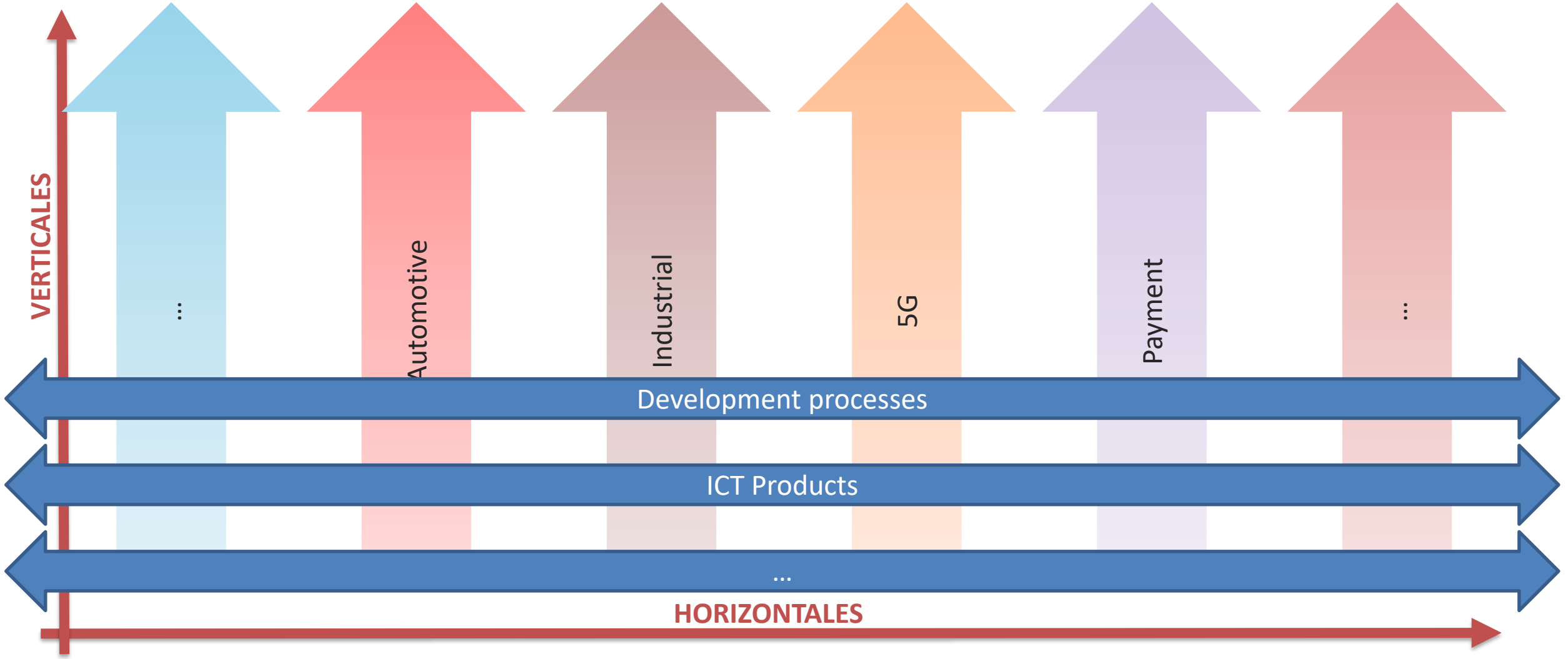
2019

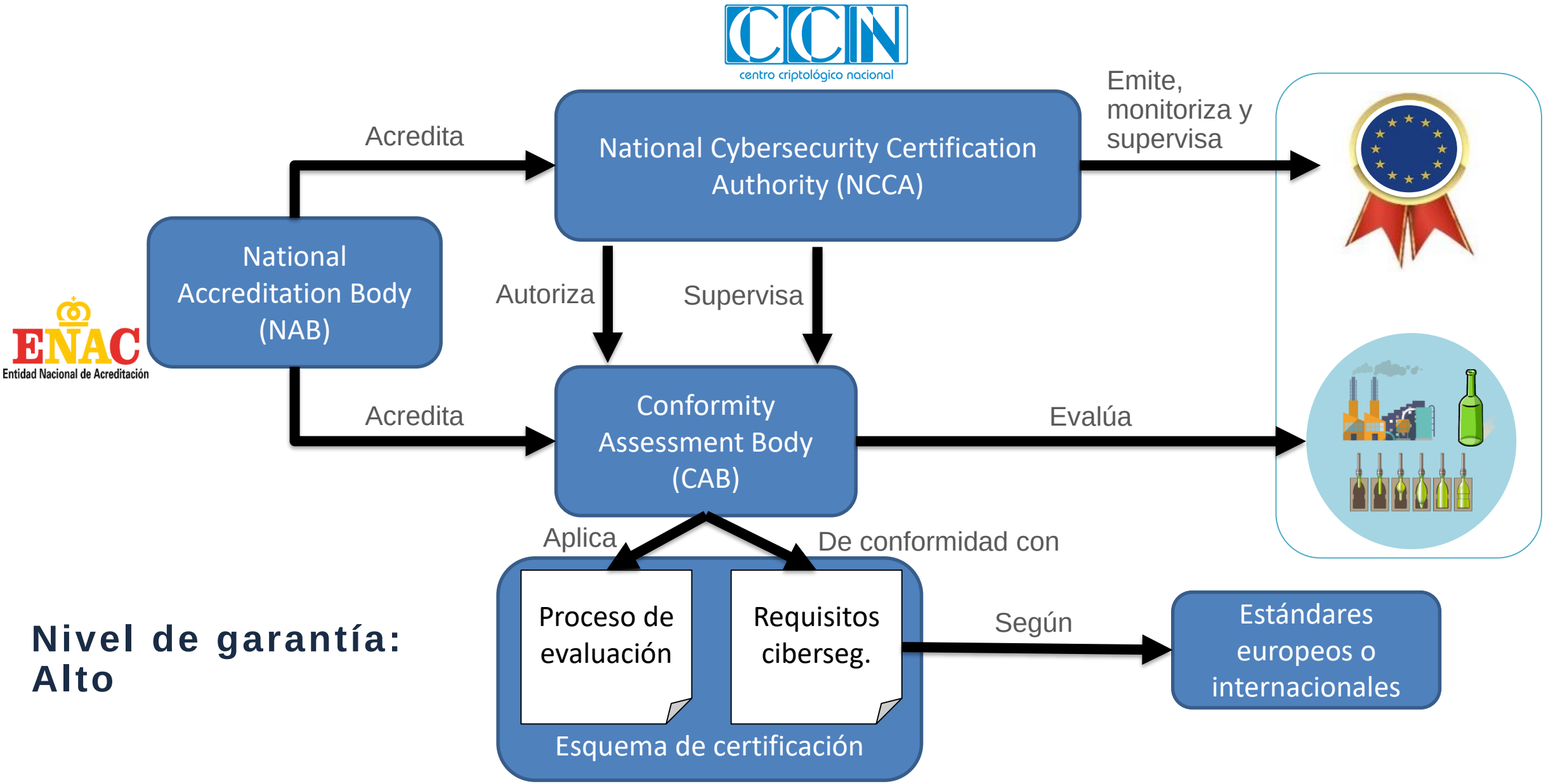
Incrementar la confianza de los usuarios respecto a los dispositivos conectados y fortalecer la industria europea de ciberseguridad.

El framework europeo de certificación y los nuevos esquemas

- **enisa 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

El framework europeo de certificación y los nuevos esquemas





Nivel de garantía: Alto

CCN
centro criptológico nacional

ENAC
Entidad Nacional de Acreditación

National Accreditation Body (NAB)

Acredita

National Cybersecurity Certification Authority (NCCA)

Autoriza

Supervisa

Acredita

Conformity Assessment Body (CAB)

Emite, monitoriza y supervisa

Evalúa

Aplica

De conformidad con

Proceso de evaluación

Requisitos ciberseg.

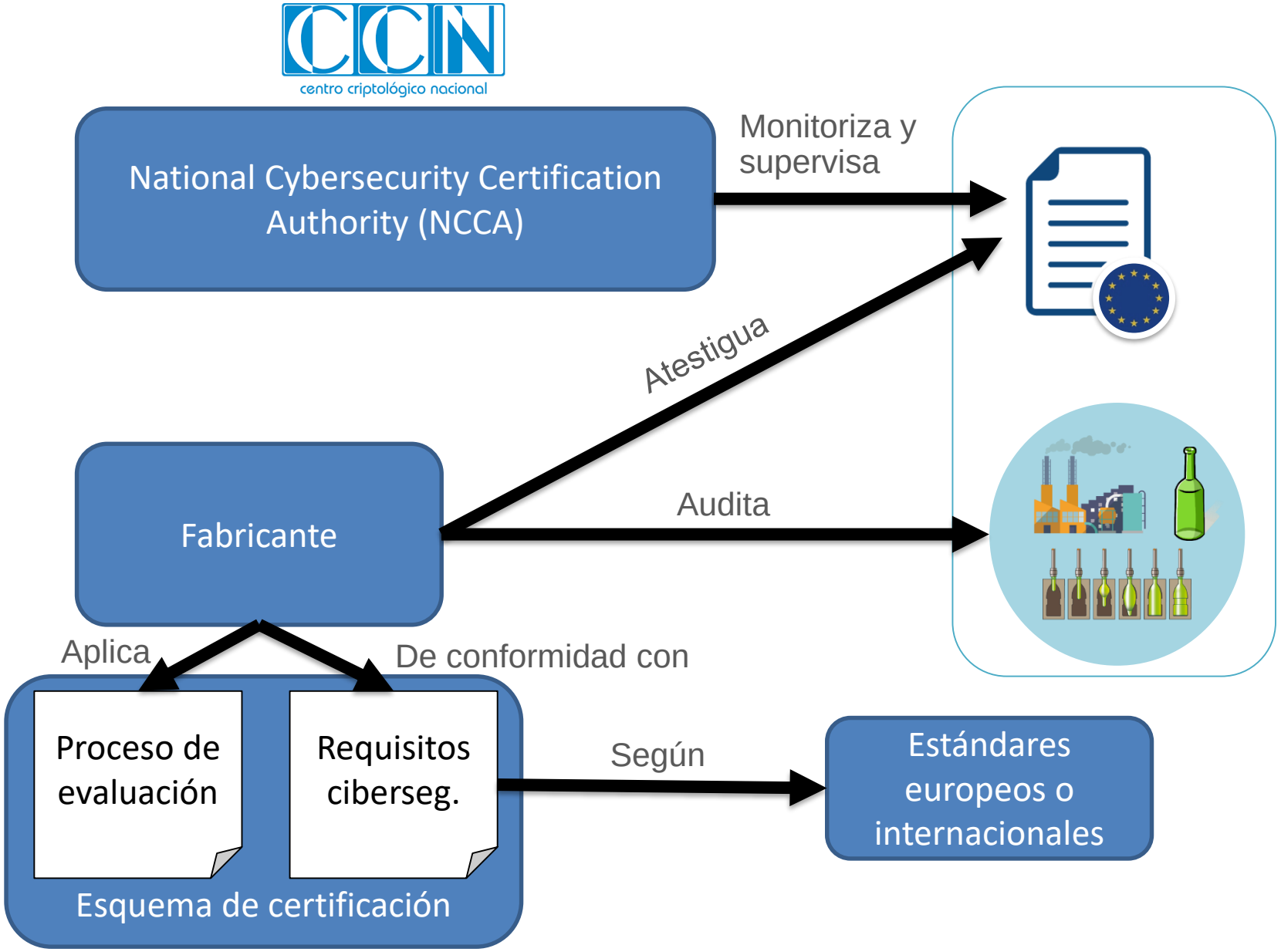
Esquema de certificación

Según

Estándares europeos o internacionales

Nivel de garantía: Substancial

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

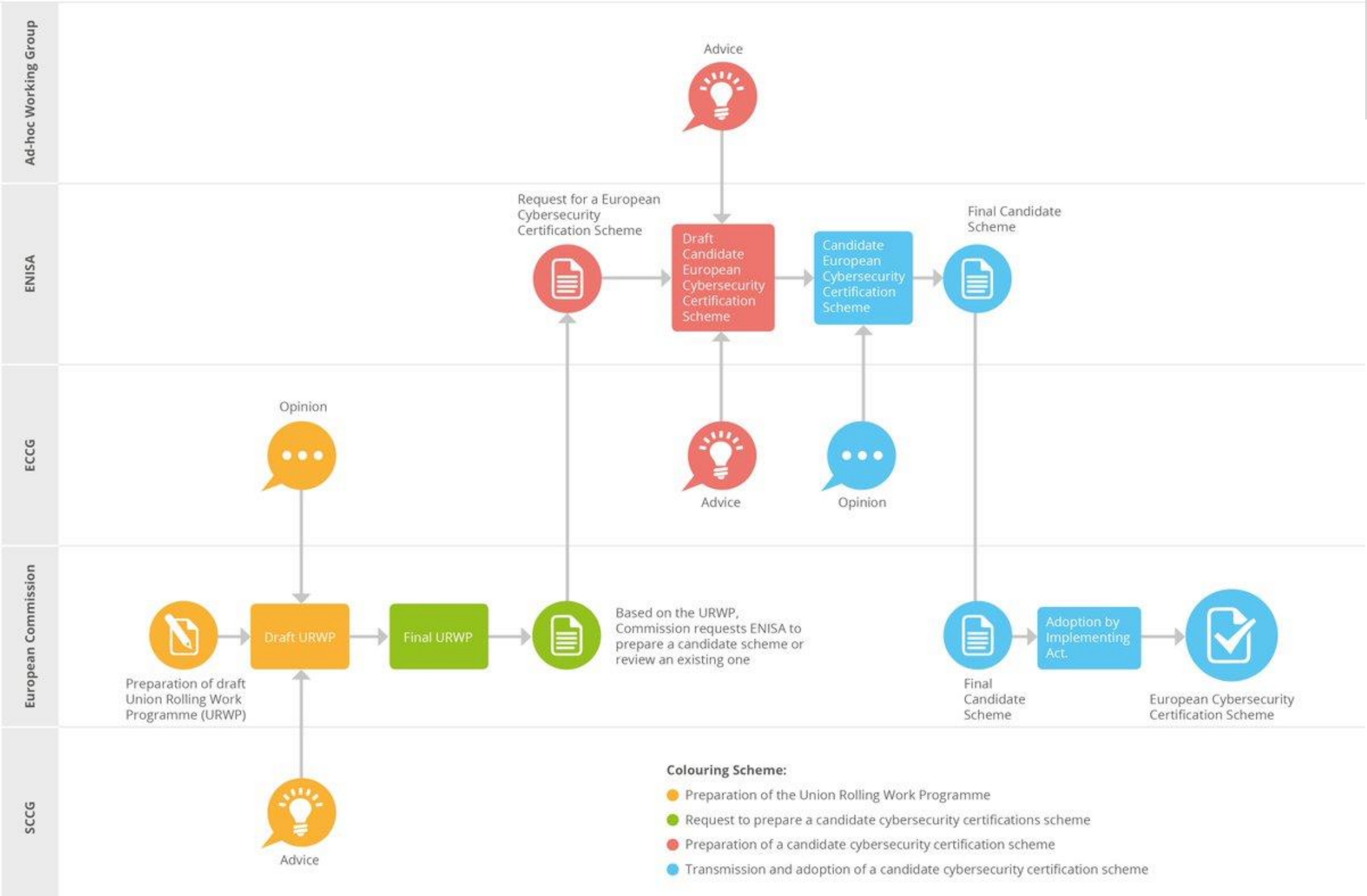
- E.g. Uso ilegítimo del certificado, no proporcionar parches de manera efectiva
- ¡Responsabilidad legal! Potenciales multas a fabricantes o CABs

Monitorización del cumplimiento

- Análisis del panorama de amenazas
- Potencialmente repetir evaluaciones

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

- Prevista revisión por la Comisión Europea en 2023


Ad-hoc Working Group
ENISA
ECCG
European Commission
SCCG
Advice
Request for a European Cybersecurity Certification Scheme
Draft Candidate European Cybersecurity Certification Scheme
Candidate European Cybersecurity Certification Scheme
Final Candidate Scheme
Opinion
Advice
Opinion
Preparation of draft Union Rolling Work Programme (URWP)
Draft URWP
Final URWP
Based on the URWP, Commission requests ENISA to prepare a candidate scheme or review an existing one
Final Candidate Scheme
Adoption by Implementing Act.
European Cybersecurity Certification Scheme
Advice
Colouring Scheme:
Preparation of the Union Rolling Work Programme
Request to prepare a candidate cybersecurity certifications scheme
Preparation of a candidate cybersecurity certification scheme
Transmission and adoption of a candidate cybersecurity certification scheme

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
  - 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

Common Criteria

El framework europeo de certificación y los nuevos esquemas

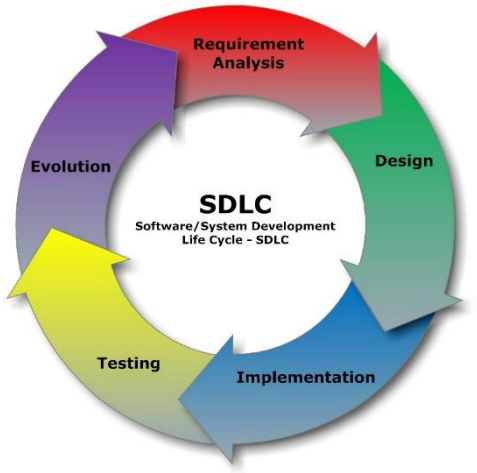
- **Servicios Cloud**
  - Esquema de certificación de **servicios** para niveles básico, substancial y alto
  - No self-assessment
  - Se lanza Adhoc WG en Marzo de 2020
  - Parte del trabajo de **CSPCert**
  - Usa el lenguaje de ISO/IEC 17788 (Infraestructura / plataforma / aplicación)
  - Metodología 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**

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
    - Servicios críticos dependerán del 5G
    - Contemplado desde la publicación de la EU Toolbox
    - Potenciales metodologías: GSMA NESAS, Common Criteria

El framework europeo de certificación y los nuevos esquemas

- Potenciales nuevos esquemas



El panorama regulatorio de la cibersalud

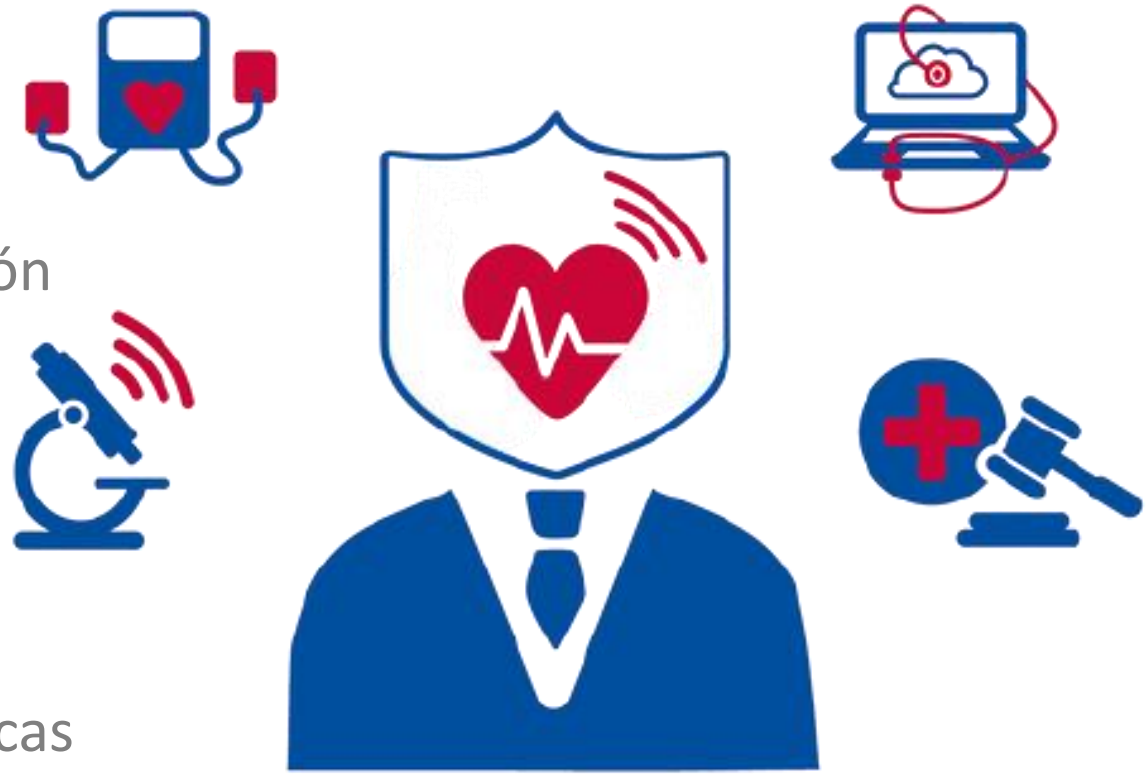
- Momento catalizador para impulsar la tecnología en eSalud
  - Seguimiento remoto: teleasistencia, localización, alarmas, seguimiento
  - Gestión asistencial: listas de espera, acceso a historial e informes clínicos, etc
  - Programas de salud: atención cardiovascular, diabetes, etc.

- Convergencia de integración de forma inteligente de lo datos recopilados por los sensores de los dispositivos médicos y de las tecnologías móviles que se utilizan en la asistencia sanitaria
  - Sistemas específicos de tecnología de la información para la atención de la salud
  - Productos médicos conectados a la red ("la Internet de los objetos médicos")

El panorama regulatorio de la cibersalud

El panorama regulatorio de la cibersalud

- Problemática del Sector Salud
  - Muy atractivo por los datos que maneja para ciberdelincuentes
    - Historiales clínicos
    - Datos personales
    - Información financiera
    - Propiedad intelectual / Investigación
  - Muchos errores humanos
  - Sistemas heredados
    - Profundamente implantados
    - Software fuera de soporte
    - Dificultad de parchear sistemas
  - Necesidad de implantar buenas prácticas
  - Ransomware y Advanced Persistant Threats (APTs)



El panorama regulatorio de la cibersalud

- Orangeworm (2018)
  - Operando desde 2015 (EEUU, Europa y Asia)
  - Objetivo: Grandes empresas internacionales y organizaciones de salud con el fin de realizar espionaje corporativo
  - También ataques contra otras empresas y sectores proveedores del sector salud.
  - No eligen a sus víctimas al azar. Seleccionan los objetivos deliberada y cuidadosamente, llevando a cabo una planificación concienzuda antes de lanzar el ataque.

El panorama regulatorio de la cibersalud

- Orangeworm (2018)
  - Carga malware en dispositivos que alojan software empleado para controlar:
    - Máquinas de rayos X
    - Resonancia Magnética Nuclear (RMN)
  - También dispositivos utilizados para ayudar a los pacientes a completar los formularios de consentimiento para procedimientos médicos.

- Espionaje industrial
  - Recientemente Vacuna española COVID-19

El panorama regulatorio de la cibersalud

- Regulaciones europeas
  - Sistemas
    - Directiva NIS
    - GDPR
  - Productos
    - Medical Device Regulation (MDR)
  - EU CyberSecurityAct

- Regulaciones americanas
  - Sistemas: HIPAA (Health Insurance Portability and Accountability Act of 1996)
  - Productos: Guía de ciberseguridad de la FDA

El panorama regulatorio de la cibersalud

- La Regulación de Dispositivos Médicos (MDR) es una nueva regulación que incluye disposiciones específicas relacionadas con la seguridad informática (hardware, software, etc.) para todos los dispositivos médicos.

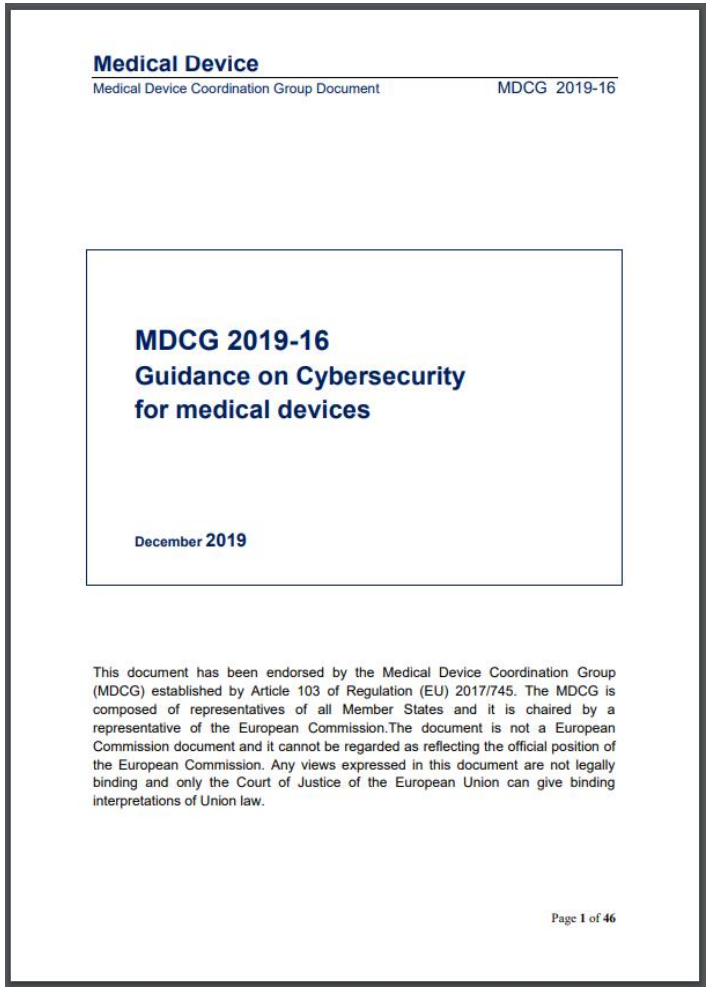
- El nuevo Reglamento de Dispositivos Médicos (MDR) 2017/745 dice: "En el caso de los dispositivos que incorporen software o de los programas informáticos que sean dispositivos en sí mismos, el software se desarrollará y fabricará de conformidad con el estado de la técnica teniendo en cuenta los principios del ciclo de vida del desarrollo, la gestión de riesgos, incluyendo la verificación y la validación de la seguridad de la información".

El panorama regulatorio de la cibersalud

- Los requisitos generales de seguridad y rendimiento definidos dentro de la MDR (Medical Devices/SW) incluyen: repetibilidad, fiabilidad y rendimiento de acuerdo con el uso previsto los principios del ciclo de vida de desarrollo, gestión de riesgos, verificación y validación el uso de software en combinación con plataformas de computación móvil las medidas de seguridad de TI, incluida la protección contra el acceso no autorizado.

- El Grupo de Coordinación de Dispositivos Médicos (MDCG) publicó la Guía sobre Ciberseguridad para dispositivos médicos 6 en diciembre de 2019 con el fin de proporcionar a los fabricantes orientación sobre cómo cumplir todos los requisitos esenciales pertinentes del MDR.

El panorama regulatorio de la cibersalud



Medical Device
Medical Device Coordination Group Document MDCG 2019-16

MDCG 2019-16
Guidance on Cybersecurity for medical devices

December 2019

This document has been endorsed by the Medical Device Coordination Group (MDCG) established by Article 103 of Regulation (EU) 2017/745. The MDCG is composed of representatives of all Member States and it is chaired by a representative of the European Commission.The document is not a European Commission document and it cannot be regarded as reflecting the official position of the European Commission. Any views expressed in this document are not legally binding and only the Court of Justice of the European Union can give binding interpretations of Union law.

Page 1 of 46

3. Secure Design and Manufacture 14
3.1. "Secure by design" 15
3.2. Security Risk Management 16
3.3. Security Capabilities 18
3.4. Security Risk Assessment 19
3.5. Security Benefit Risk Analysis 19
3.6. Minimum IT Requirements 20
3.7. Verification/Validation 22
3.8. Lifecycle Aspects 23
4. Documentation and Instructions for use 23
4.1. Documentation 23
4.2. Instructions for use 24
4.3. Information to be provided to healthcare providers 27
5. Post-Market Surveillance and Vigilance 28
5.1. Post-market surveillance system 28
5.2. Vigilance 29

El panorama regulatorio de la cibersalud

- A nivel de sistemas:
  - Trasladar requisitos de seguridad a proveedores
  - Uso de proveedores certificados
    - EU cybersecurity certification schemes, if applicable
    - Servicios (e.g. 27001)
    - Productos (Medical Device Regulation)

  - https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

Contacto

jtsec: Beyond IT Security

Granada & Madrid – Spain

hello@jtsec.es

@jtsecES

www.jtsec.es

“Any fool can make something complicated. It takes a genius to make it simple.”
Woody Guthrie