aCtive sEcurity foR connecTed devIces liFecYcle

CERTIFY

AIR Institute

July 3rd, 2025.

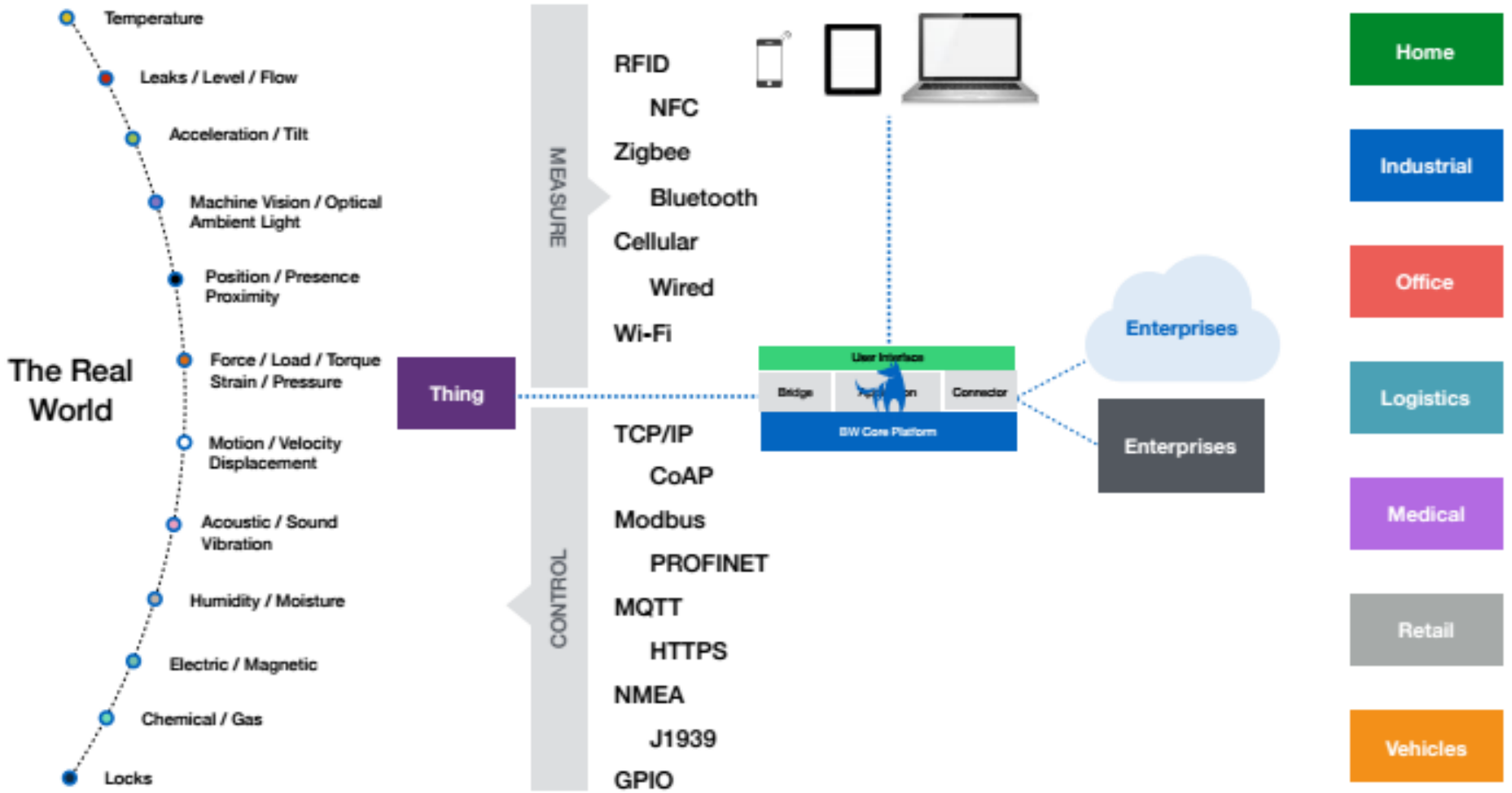
The CERTIFY project has received funding from the European Union's HE research and innovation programme under the grant agreement No. 101069471 and from the Swiss SERI's under grant agreements No. 22.00165 and 22.00191. The European Commission's and Swiss SERI's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views of the authors only, and neither the Commission nor the Swiss Confederation can be held responsible for any use which may be made of the information contained therein.

aCtive sEcurity foR connecTed devIces liFecYcles

(Seguridad activa para el ciclo de vida de dispositivos conectados)

- Horizon EU CERTIFY https://certify-project.eu/ (13 socios de 8 países, del 1 de octubre de 2022 al 30 de septiembre de 2025).
- Tiene como objetivo proponer una metodología y un marco para la gestión de la ciberseguridad de dispositivos del Internet de las Cosas (IoT) durante todas las etapas de su ciclo de vida, ofreciendo:
  - (Re)certificación y evaluación de seguridad apoyadas en evidencias proporcionadas por la configuración segura más reciente del dispositivo especificada por el fabricante.
  - Registro, aprovisionamiento y despliegue seguros mediante la (re)configuración automática de dispositivos IoT.
  - Mejora de la seguridad del hardware abierto mediante la aplicación de principios de diseño seguro ("secure-by-design") para el aprovisionamiento de claves, almacenamiento seguro, arranque seguro y cifrado (gracias a entornos de ejecución confiables hardware/software y elementos seguros).
  - Evaluación de seguridad en el arranque y en tiempo de ejecución mediante perfiles de comportamiento para un análisis continuo del dispositivo y la red.
  - Monitorización de seguridad, detección y reacción oportuna (incluidas actualizaciones) frente a un panorama de amenazas en constante evolución.
  - Intercambio de información de manera segura, preservando la privacidad y generando confianza entre todas las partes interesadas.

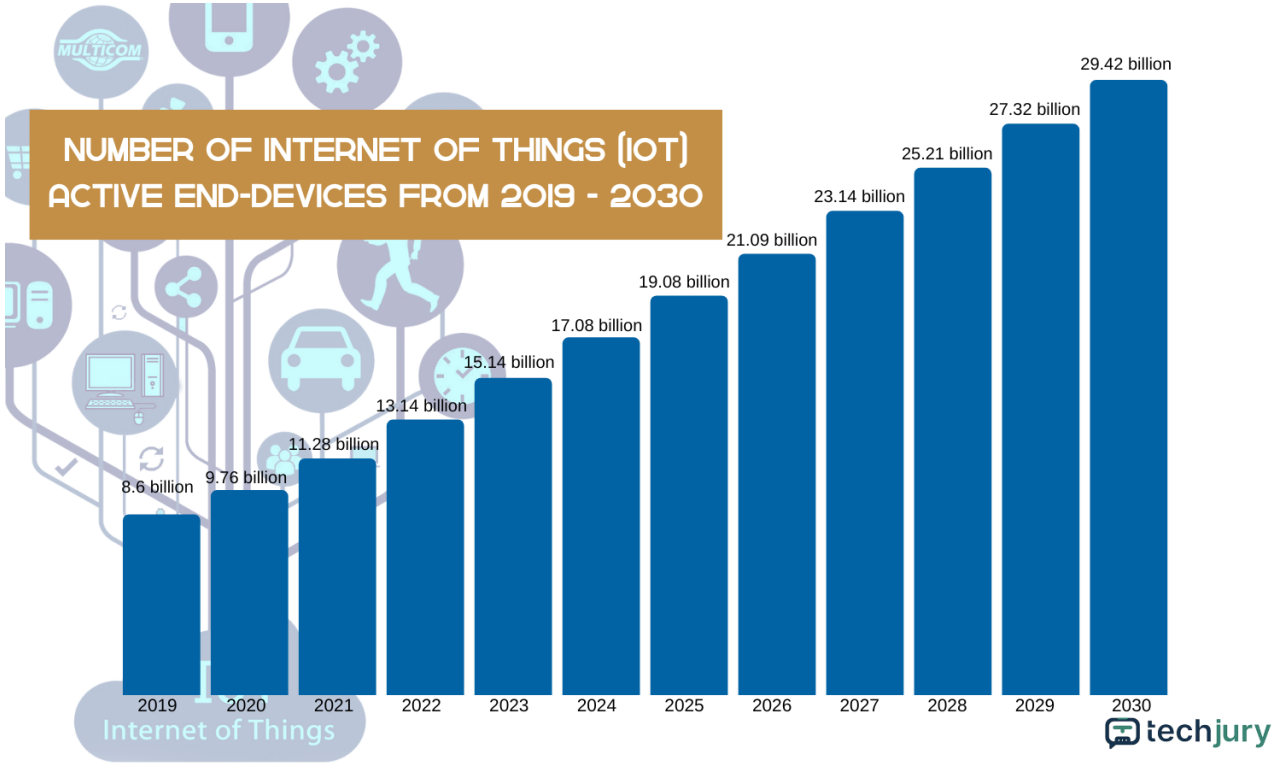
The Internet of Things



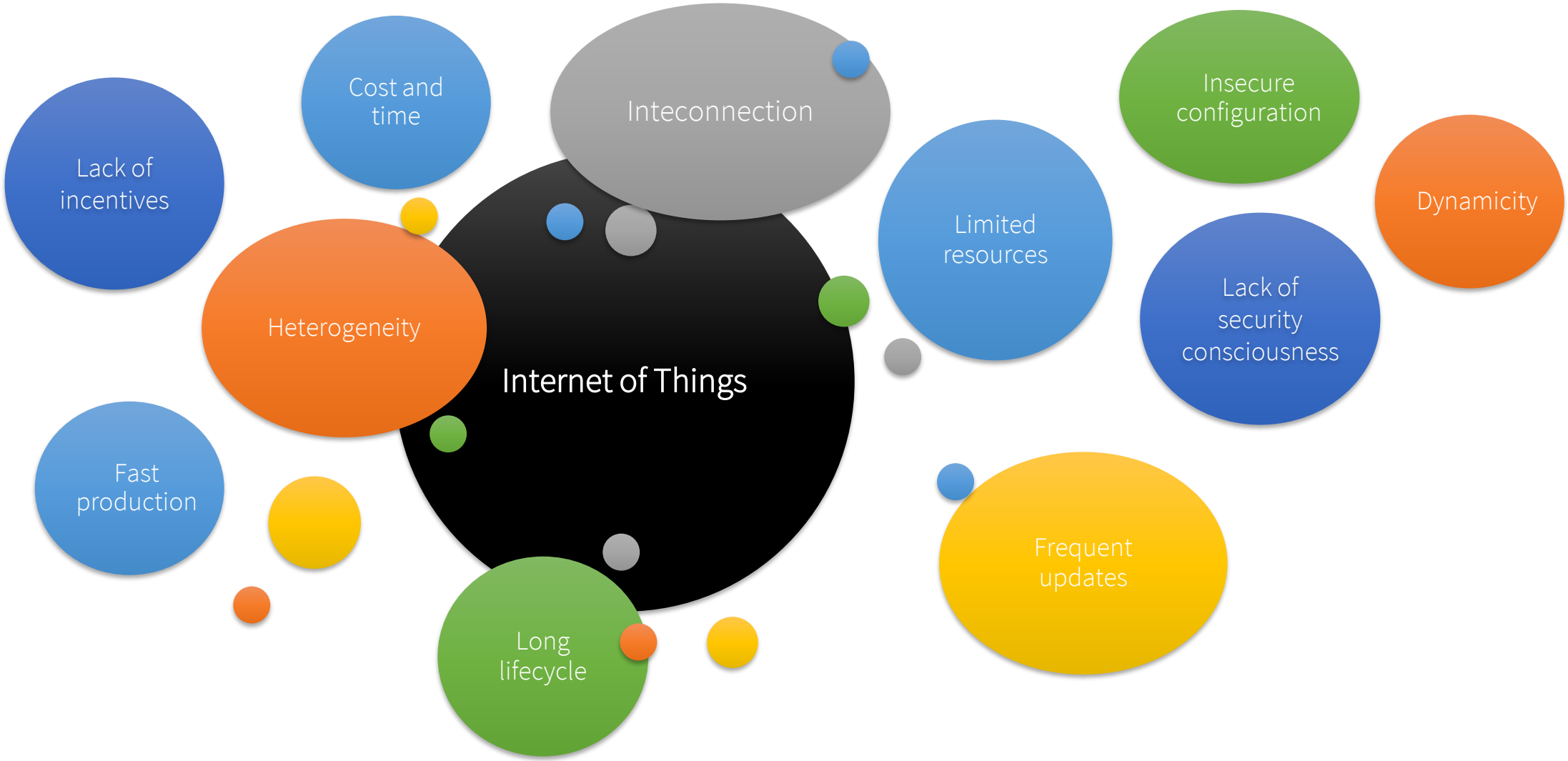
El Internet of Things en numeros

- Cada minuto, 7.620 nuevos dispositivos IoT se conectan a Internet.
- El número de dispositivos IoT disponibles aumentará significativamente cada año, alcanzando los 30 mil millones para 2030.
- La integración del IoT en los procesos empresariales ha mejorado la eficiencia hasta en un 83%.
- Para 2028, se estima que el mercado del IoT en el sector automotriz alcanzará los 882.000 millones de dólares.

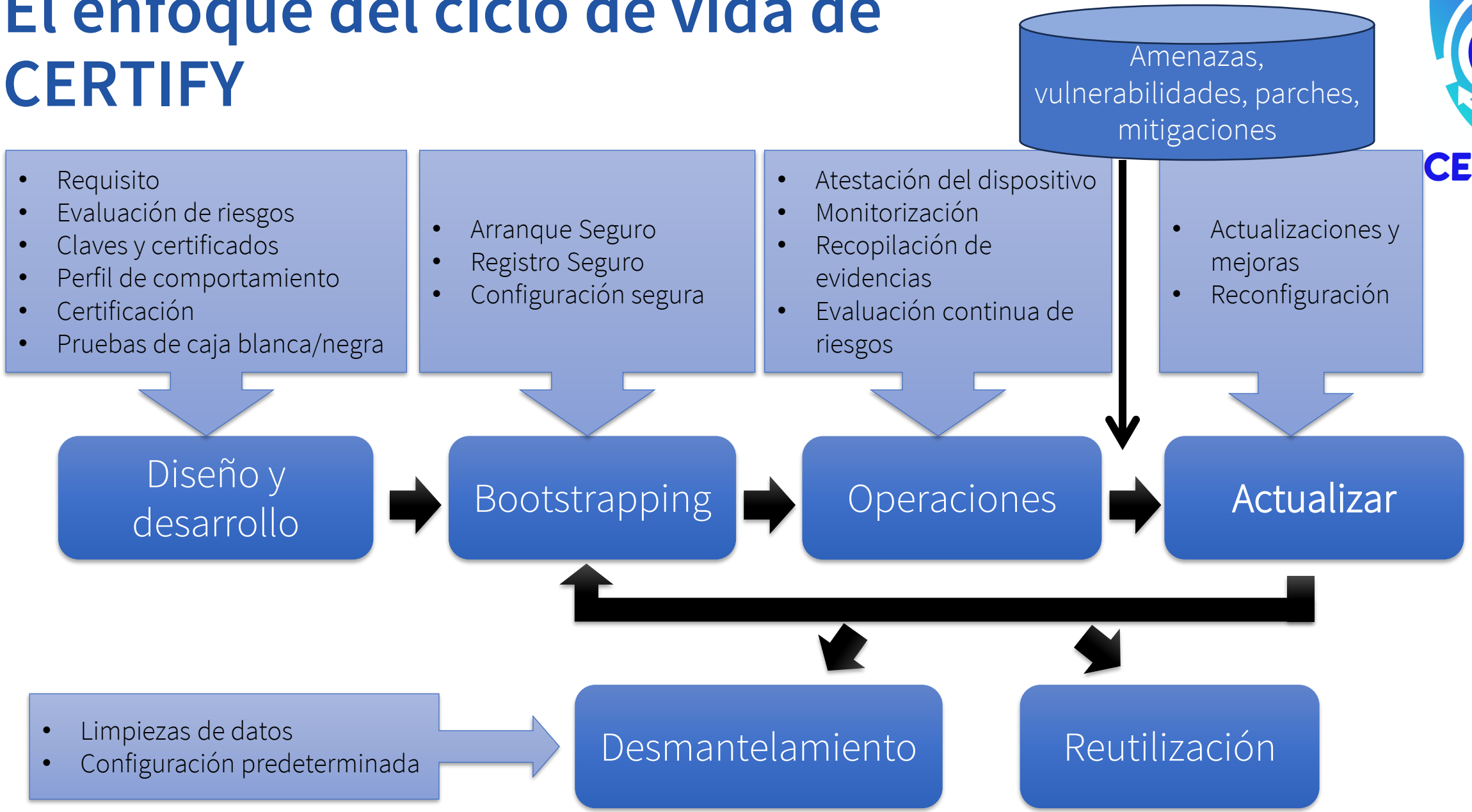
- En 2016, la botnet Mirai infectó más de 600.000 dispositivos IoT vulnerables. Servicios y sitios web importantes, como Spotify, Netflix y PayPal, quedaron temporalmente fuera de servicio. OVH informó que estos ataques superaron 1 Tbps, siendo los mayores registrados públicamente.
- En 2017, VPNFilter infectó más de medio millón de routers en más de 50 países. Puede instalar malware en los dispositivos conectados al router, interceptar y recopilar información transmitida, bloquear el tráfico de red y robar contraseñas.



IoT lifecycle management challenges



El enfoque del ciclo de vida de CERTIFY

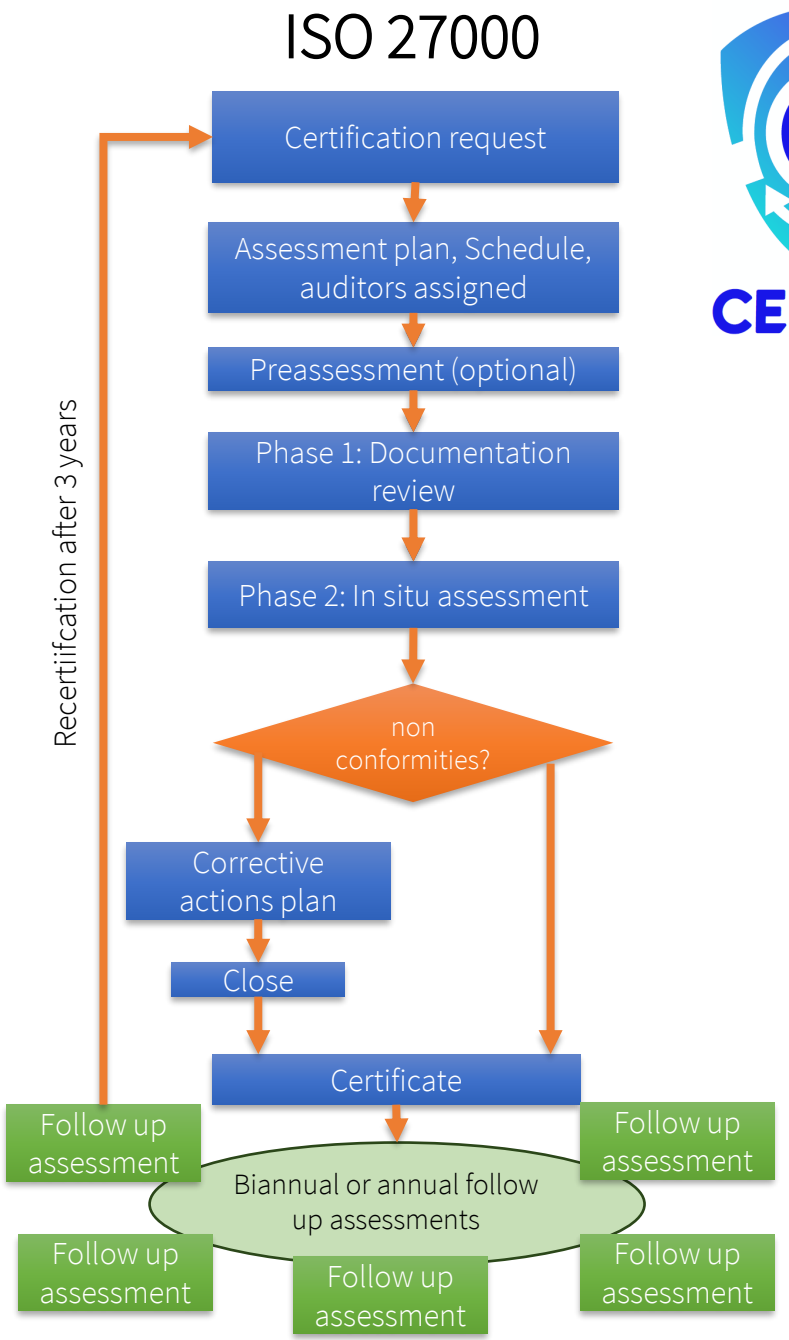


Diseño y desarrollo: Normas y certificaciones de ciberseguridad

- Definición de casos de uso con un enfoque en la seguridad, identificando los requisitos de seguridad.
- **Modelado de amenazas:** analizar la aplicación desde la perspectiva de un posible atacante, identificando cómo podría explotarla y cómo prevenirlo.
- Identificación de directrices, normas de seguridad y regulaciones aplicables.
  - ETSI EN 303 645
- Evaluación de riesgos y pruebas considerando el dominio de aplicación objetivo.
  - Uso de herramientas DAST, SAST, SCA para pruebas de caja negra y blanca.
- **Certificación**

Diseño y desarrollo: Normas y certificaciones de ciberseguridad

- La certificación es una evaluación integral de un componente TIC, que determina hasta qué punto un diseño e implementación específicos cumplen con los requisitos de seguridad establecidos.
- La certificación es realizada por un Organismo de Evaluación de la Conformidad (CAB, por sus siglas en inglés), que puede llevar a cabo auditorías y/o pruebas.

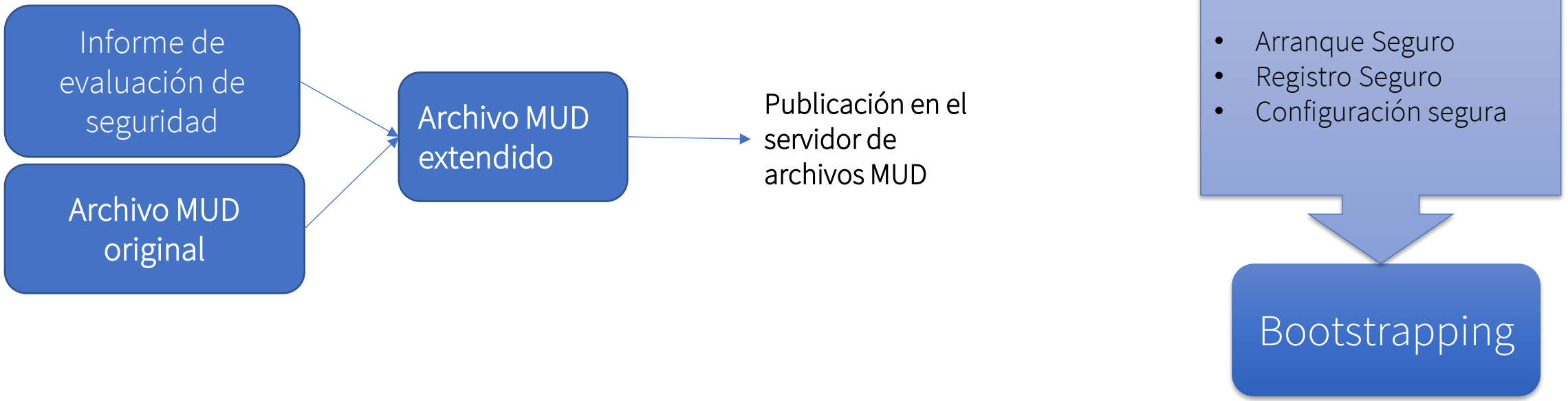


Diseño y desarrollo: Normas y certificaciones de ciberseguridad

- Definición de casos de uso con un enfoque en la seguridad, identificando los requisitos de seguridad.
- Modelado de amenazas: analizar la aplicación desde la perspectiva de un posible atacante, identificando cómo podría explotarla y cómo prevenirlo.
- Identificación de directrices, normas de seguridad y regulaciones aplicables.
- Evaluación de riesgos y pruebas considerando el dominio de aplicación objetivo.
- Uso de herramientas **DAST, SAST y SCA** para pruebas de caja negra y blanca.
- Certificación.
- Perfil de comportamiento.
- Aprovisionamiento de claves y certificados.

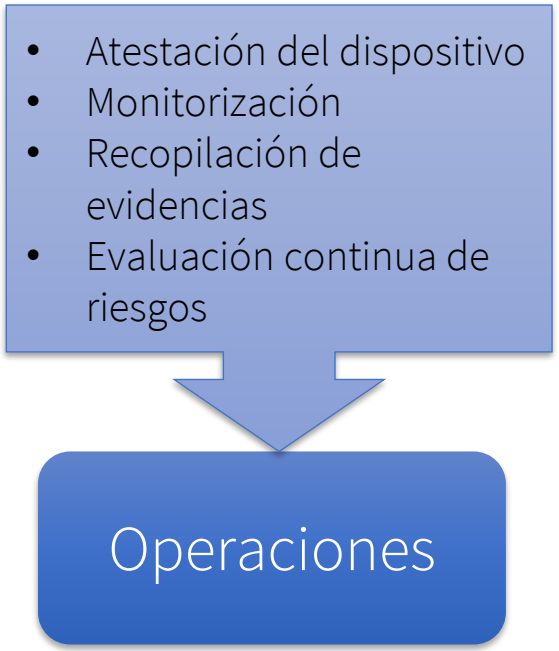
Inicio seguro (Bootstrapping): Despliegue seguro

1. Autenticación segura y derivación de material criptográfico basada en EAP-AAA
2. Recuperación de MUD (extensión del estándar de IETF)
3. Aplicación de políticas MUD para una configuración segura
4. Atestación DAA como condición para un inicio seguro exitoso



Atestación en tiempo de ejecución y monitorización

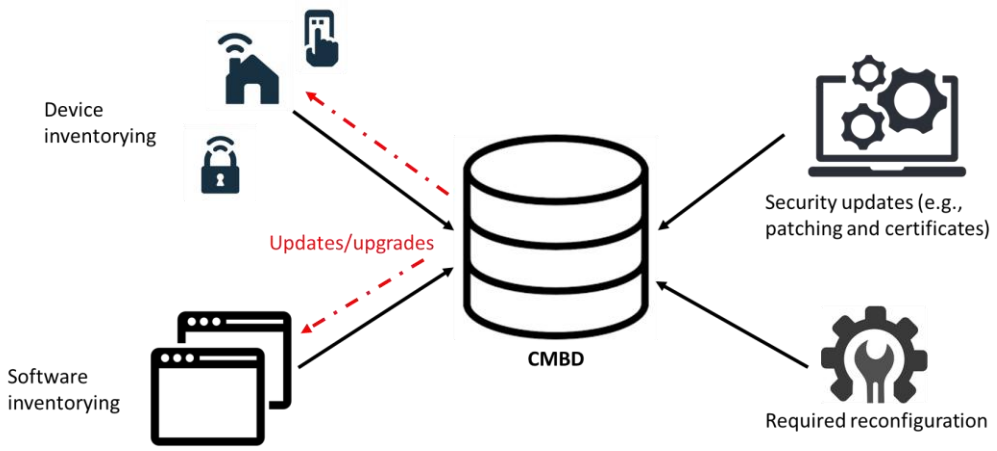
- **Runtime attestation and monitoring**
  - Herramientas SIEM (Gestión de Información y Eventos de Seguridad) que proporcionan correlación de información de seguridad desde diversas fuentes, como Elastic. https://www.gartner.com/reviews/market/security-information-event-management
  - Sistemas de Detección de Intrusos (IDS)
- **Compartición de Inteligencia de Amenazas Cibernéticas (CTI):** compartir información identificada es crucial para responder a los ataques lo antes posible.
  - Estándares, formatos y protocolos comunes: STIX, CybOX, TAXII
  - Plataformas que facilitan la colaboración e intercambio de CTI: MISP
  - Compartición de información sensible preservando la privacidad
  - Acciones de mitigación → Threat MUD
- Evaluación continua usando métricas en tiempo de ejecución y evidencias → **Recertificación**



•Reconfiguración

Actualización: Actualizaciones OTA y gestión del ciclo de vida

- Protección de las imágenes de software: solo proveedores legítimos y autorizados, garantizando la integridad del sistema y previniendo ataques de reversión.
- Mecanismos de seguridad eficientes adecuados para dispositivos y redes con recursos limitados.
- Las tecnologías de registros distribuidos (DLT) proporcionan un libro de registro transparente para gestionar las diferentes versiones de los elementos de software.



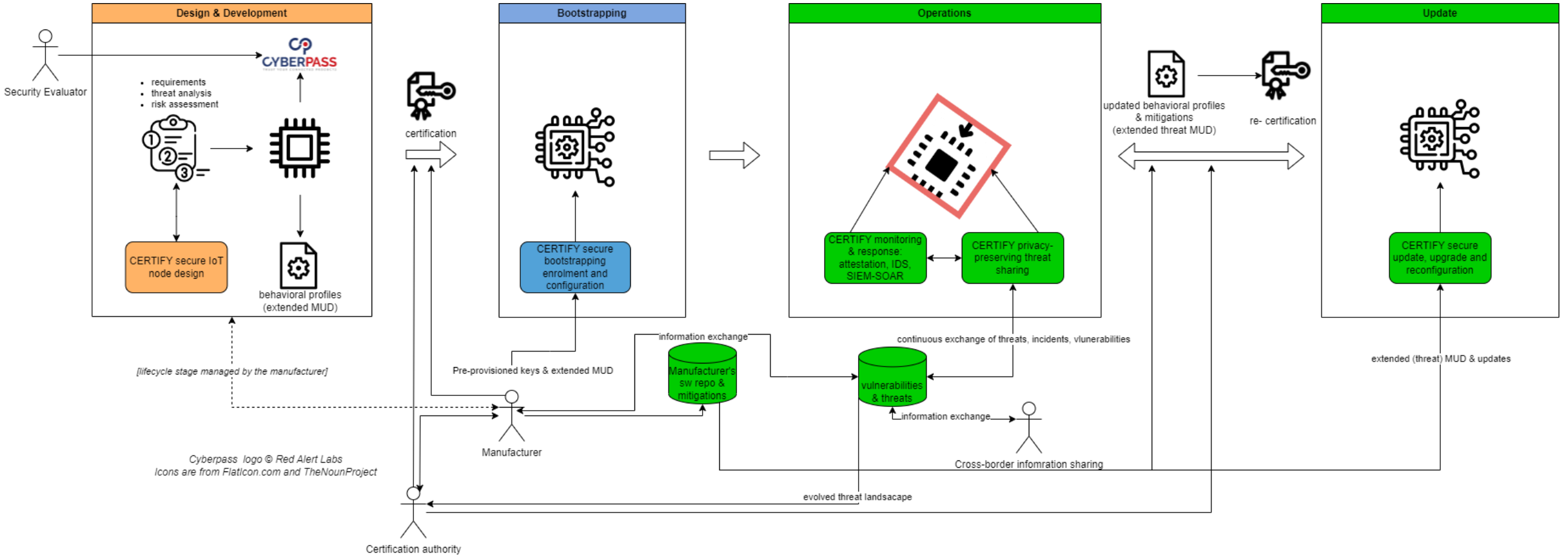
- Actualizaciones y mejoras
- Reconfiguración

Update

Desmantelamiento seguro o retiro seguro del servicio

- **Reutilización (Repurposing):** Se identifica un subsistema con diferentes requisitos de ciberseguridad y el dispositivo puede ser reutilizado para cumplir con su nuevo rol.
  - El dispositivo se reconfigura antes de su reutilización, lo que ofrece una oportunidad de ahorro de costes.
- **Desmantelamiento (Decommissioning):** El dispositivo ya no puede cumplir con el nivel de garantía requerido por el dominio, o el proceso de mitigación sugerido no puede llevarse a cabo.
  - Asegurar que no se filtre información previamente almacenada.
  - Aplicar políticas de limpieza.
- **La desinfección de datos puede realizarse mediante métodos de borrado por software o destrucción física de los componentes de almacenamiento.**
- El dispositivo debe ser restaurado a la configuración predeterminada de fábrica.
- Si es necesario, desmontar cuidadosamente el dispositivo para separar los componentes reutilizables de aquellos que deben ser desechados. Manipular materiales peligrosos (como baterías) con precaución.

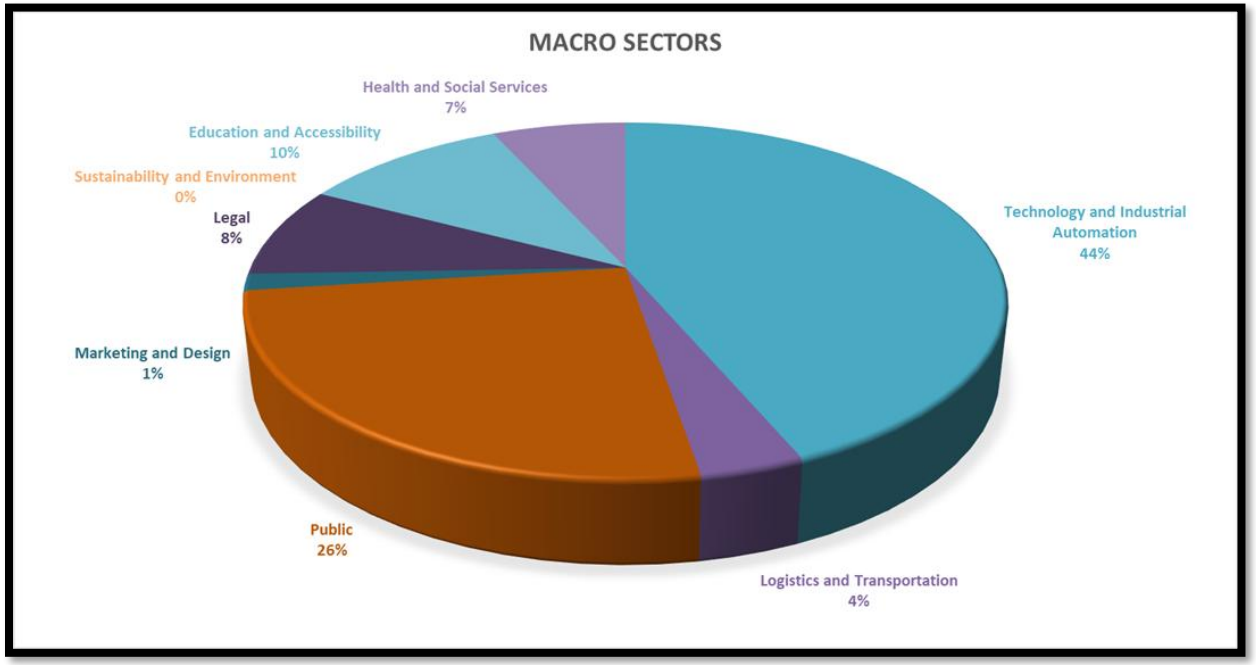
Hacia una recertificación continua en el ciclo de vida de CERTIFY



Conclusiones clave

- Los dispositivos IoT mejoran enormemente nuestras vidas al conectar y automatizar múltiples aspectos, pero también representan riesgos significativos de ciberseguridad que deben gestionarse cuidadosamente.
- Los dispositivos IoT requieren una gestión de la ciberseguridad cuidadosa y flexible durante todo su ciclo de vida.
- Tal como destacan las últimas regulaciones europeas (CSA y CRA), crear un entorno digital de confianza requiere certificación y una gestión completa del ciclo de vida.
- CERTIFY proporciona un marco para gestionar la seguridad durante todo el ciclo de vida del IoT, asegurando que los dispositivos certificados mantengan su nivel de garantía durante toda su vida útil. Incluye:Security by design support
    - Soporte para seguridad desde el diseño (security by design)
    - Evaluación y monitorización continua de la seguridad
    - Detección oportuna, mitigación y reconfiguración
    - Actualización y mejora segura de los dispositivos IoT
    - Compartición continua de información de seguridad

Certify comunidad



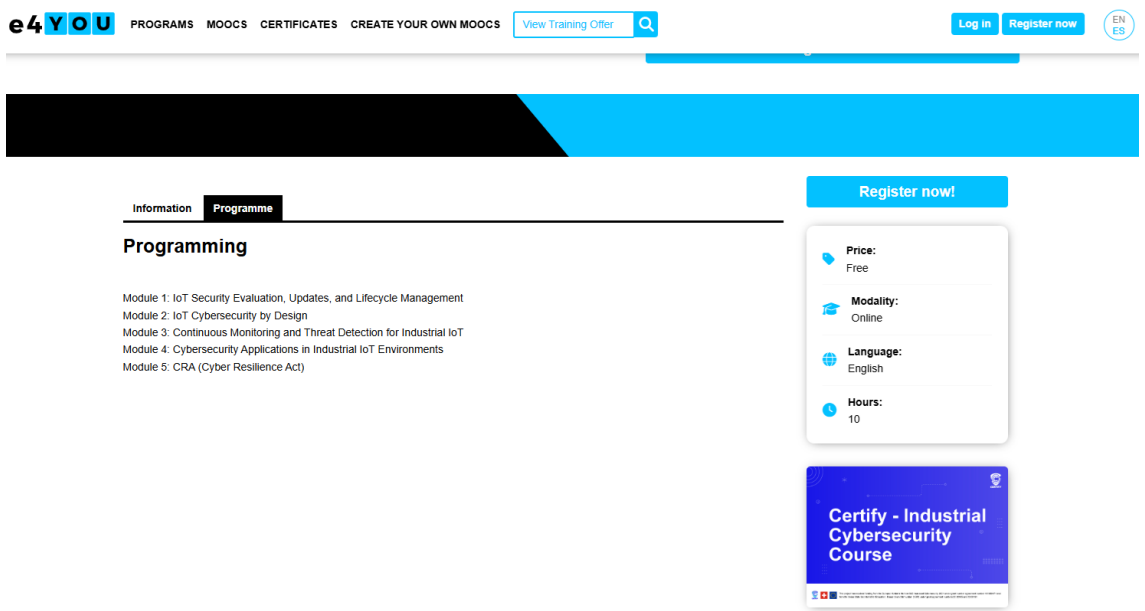
296 Participants

- Tecnología y Automatización Industrial: 44%
- Sector Público: 26%
- Educación y Accesibilidad: 11%
- Legal: 8%
- Salud y Servicios Sociales: 7%
- Logística y Transporte: 4%
- Marketing y Diseño: 2%

Sobre el Curso

CONTENIDO

Este curso, impartido por académicos e investigadores europeos, consta de cinco módulos que abordan una variedad de temas. Entre ellos se incluyen la integración de la seguridad en dispositivos IoT, la detección de amenazas en entornos industriales, la evaluación continua de las operaciones de IoT y la comprensión de los procesos de certificación requeridos a lo largo de su ciclo de vida.



About the Course

Metodología

- 100% online (hasta el 31 de julio de 2025).
- Tras revisar los cinco módulos, los participantes recibirán un certificado que acredita 10 horas de asistencia.

Registraros en: https://e4you.org/en/moocs/certify-industrial-cybersecurity

This project has received funding from the European Union's Horizon CL3 Increased Cybersecurity 2021 under grant number agreement number 101069471 and from the Swiss State Secretariat for Education, Research and Innovation (SERI) under grant agreement numbers 22.00165 and 22.00191

Gracias

- Síguenos en: https://certify-project.eu/