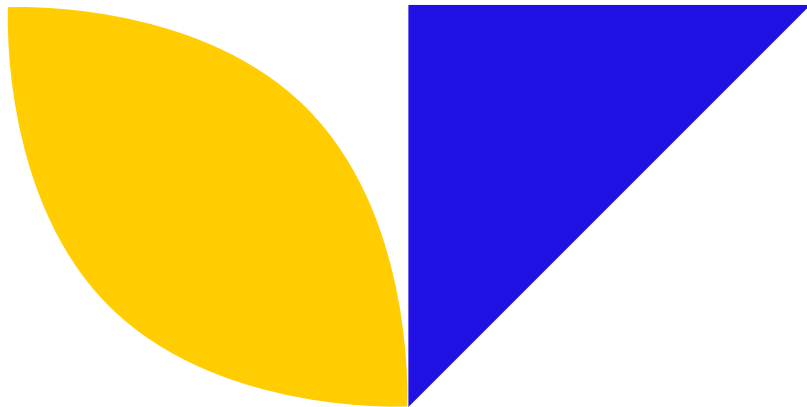
Módulo 1.

Tendencias tecnológicas emergentes: innovación e impacto

Parte 2

GENERACIÓN D · UNIÓN PROFESIONAL · Upro
Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL · red.es
Plan de Recuperación, Transformación y Resiliencia

ÍNDICE



05

Cloud Computing y datos a escala

Modelos de servicio, arquitecturas cloud-native y plataformas de datos para IA

Cloud Computing y datos a escala

¿Qué vamos a trabajar en esta unidad?

Modelos de servicio: IaaS, PaaS, SaaS.

Arquitecturas cloud-native: VMs, contenedores, serverless.

Edge computing y decisiones de despliegue.

De Big Data a Lakehouse y Data Mesh.

Pipelines modernos y gobierno del dato.

Caso integrador: arquitectura de datos en la nube.

Cloud Computing y datos a escala

Modelos de servicio: IaaS, PaaS, SaaS

IaaS

La nube te da **infraestructura** (VMs, red, disco). Tú gestionas SO y aplicaciones.

Ejemplo: alquilar máquinas virtuales en la nube y montar ahí tu servidor.

PaaS

La nube te da una **plataforma gestionada**. Tú subes tu código.

Ejemplo: subir una aplicación y que la plataforma se encargue de ejecutarla, escalarla y mantener el entorno.

SaaS

La nube te da la **aplicación completa**. Tú simplemente la usas.

Ejemplo: Gmail, Salesforce, Microsoft 365, Dropbox.

Cloud Computing y datos a escala

VMs, contenedores y serverless: modelos de ejecución

- **Máquinas virtuales (VMs)**: más control y aislamiento, pero más carga operativa.
- **Contenedores**: despliegues ligeros y portables, muy útiles en microservicios y automatización.
- **Serverless**: ejecución por eventos y pago por uso, con alta abstracción de la infraestructura.

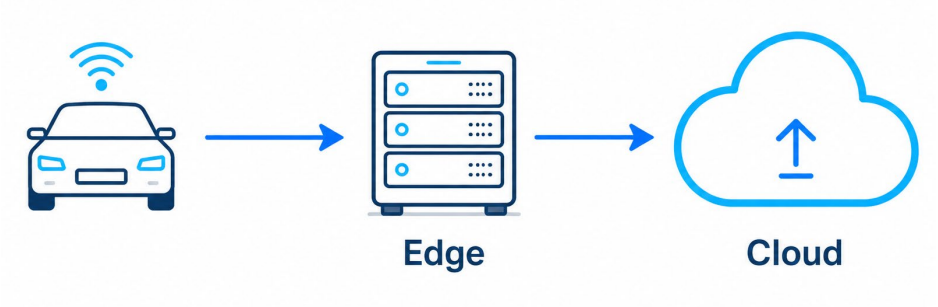
Cloud Computing y datos a escala

Edge computing y nube distribuida

Procesar datos **cerca de donde se generan** (fábrica, vehículo, tienda física).

Reducir latencia y tráfico hacia la nube.

Decidir qué corre en el borde y qué corre en la nube es una decisión arquitectónica clave.



Cloud Computing y datos a escala

De Big Data a Lakehouse y Data Mesh

01

Big Data · foco en volumen, velocidad y variedad; clústeres batch masivos.

02

Data Lake + Data Warehouse · datos crudos en el lago, datos curados para analítica.

03

Lakehouse y Data Mesh · combinar flexibilidad de lago con estructura de almacén y ownership por dominio.

04

La arquitectura evoluciona para alinear tecnología, rendimiento y cómo se organizan los equipos.

Fuente: https://learn.microsoft.com/en-us/azure/databricks/lakehouse-architecture/deployment-guide/delta-lake

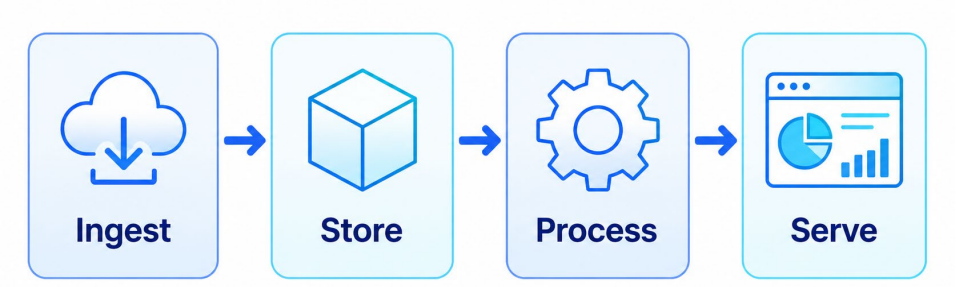
Cloud Computing y datos a escala

Pipelines modernos y gobierno del dato

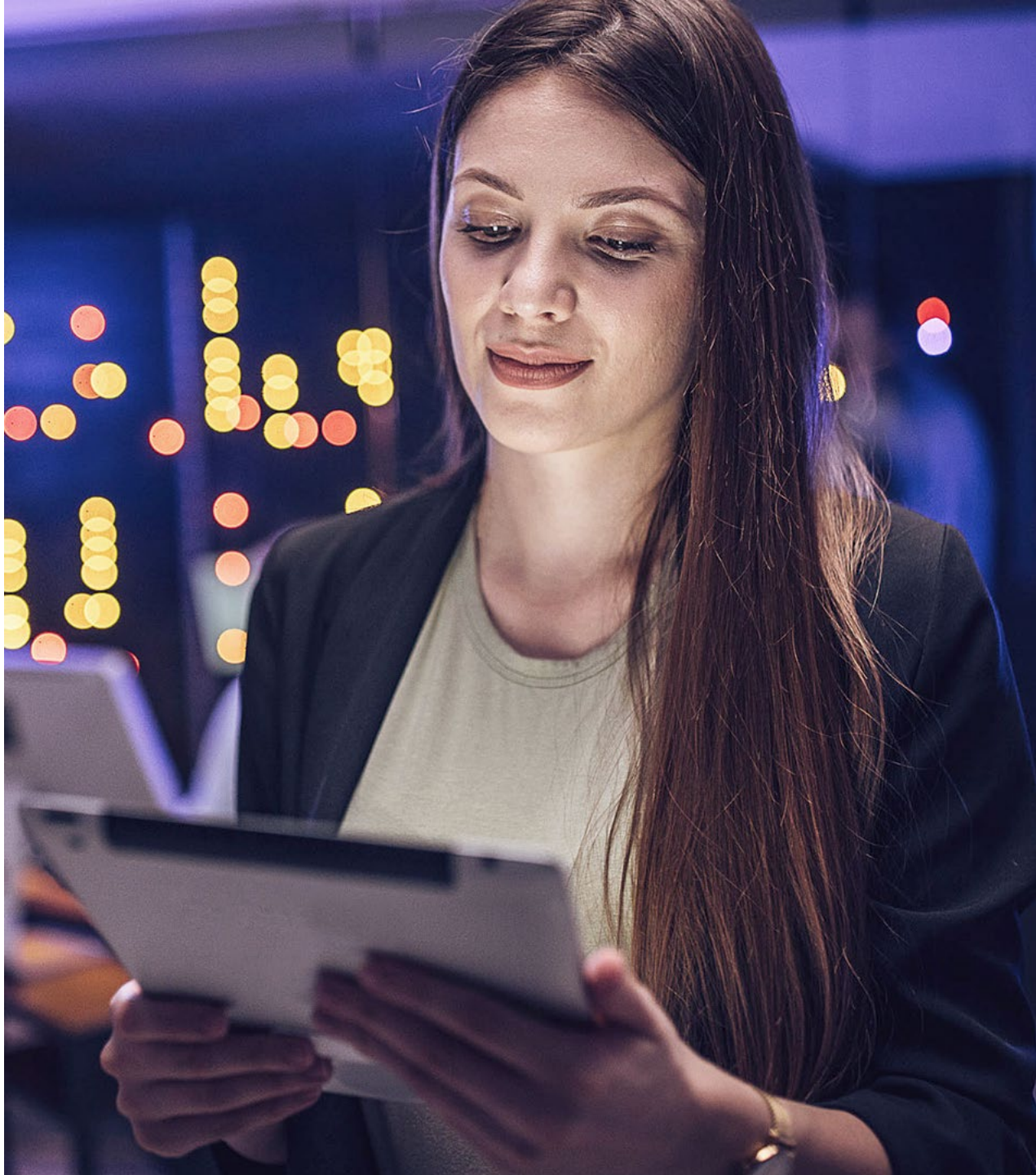
Pipeline típico: ingestión → almacenamiento → procesamiento → consumo (BI, APIs, IA).

Gobierno del dato:

- Propietarios claros, catálogo y linaje.
- Controles de calidad y de acceso.



Sin pipelines ni gobierno, la IA se construye sobre arena.



Cloud Computing y datos a escala

Actividad integradora – Arquitectura de datos en la nube

Grupos de 3–4 personas.

- Empresa digital: web + app, facturación, soporte y logs técnicos.
- Quiere dashboards casi en tiempo real y casos de IA (recomendaciones, anomalías).

Tarea

- Listad fuentes de datos y decidid si serían batch o streaming.
- Proponed dónde guardar datos crudos y curados (lake / warehouse).
- Indicad qué procesos serían batch y cuáles casi en tiempo real.
- Identificad un riesgo principal (coste, soberanía o seguridad) y cómo lo abordaríais.

No buscamos la arquitectura perfecta, sino decisiones justificadas para este contexto.

06

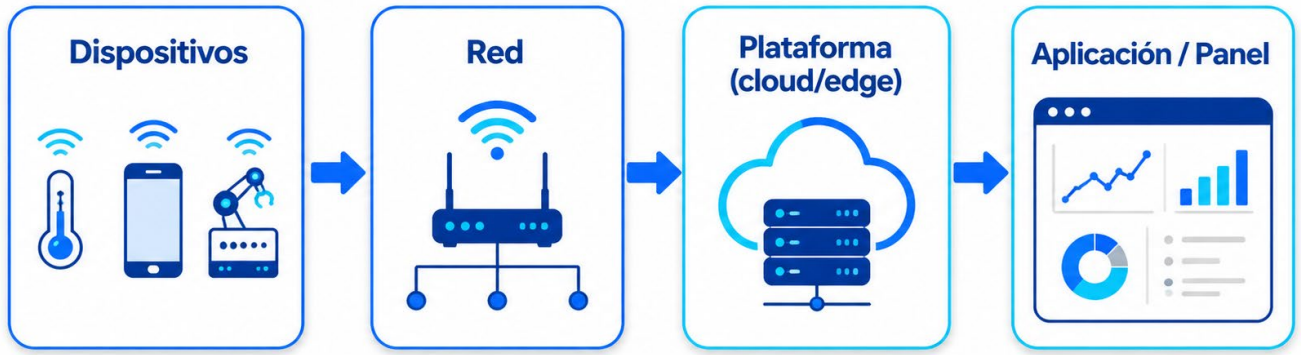
Internet of Things

Dispositivos conectados, edge, 5G e IA en sistemas IoT

Internet of Things

Arquitectura básica IoT

- Dispositivos y sensores que capturan datos del entorno.
- Redes que los conectan (Wi-Fi, 5G, LPWAN, etc.).
- Plataformas en la nube o en edge que procesan y almacenan.
- Aplicaciones que muestran información y permiten actuar.



Un sistema IoT es un "tubo" de datos: del mundo físico al mundo digital y de vuelta.

Internet of Things

Casos de uso IoT

IIoT
Sensores en máquinas para mantenimiento predictivo en fábrica.

Smart Cities
Gestión de tráfico, alumbrado, residuos, calidad del aire.

Salud conectada
Wearables que monitorizan constantes y envían datos a la nube.

Hogar inteligente
Clima, iluminación y seguridad gestionados desde el móvil.

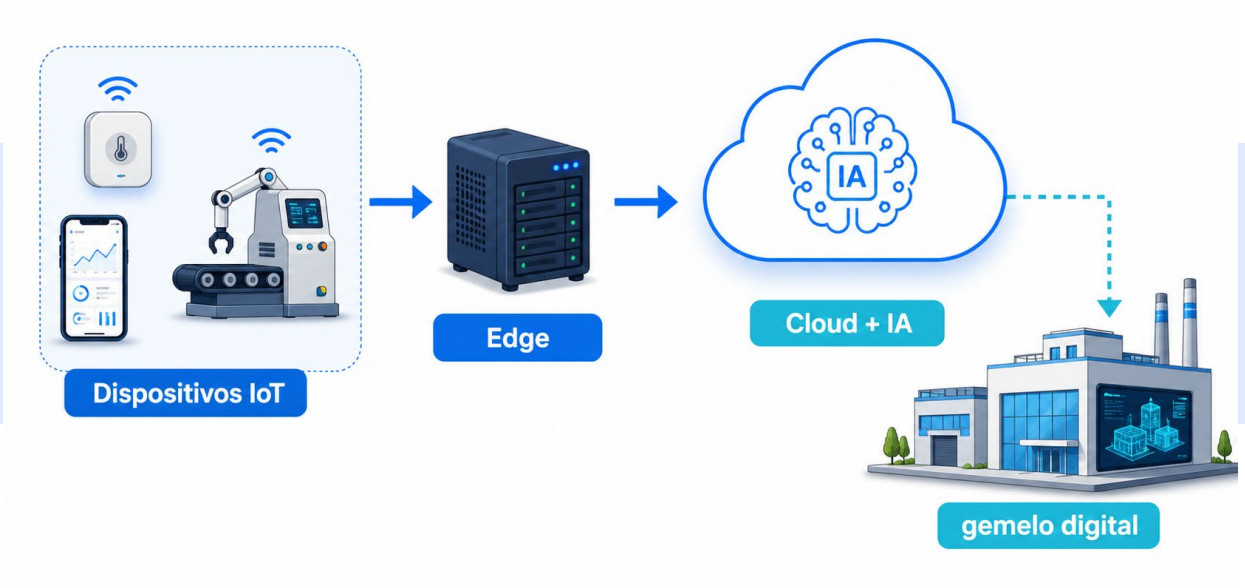
No es solo "gadgets": es infraestructura crítica conectada.

"Elegid uno de estos casos (fábrica, ciudad, salud, hogar). ¿Qué pasaría si los datos se manipulan o se filtran?"

Internet of Things

Convergencia IoT + IA + 5G + Edge

- IA en el borde: detectar anomalías y tomar decisiones cerca del dispositivo.
- 5G: más dispositivos conectados, baja latencia, más datos en tiempo real.
- Gemelos digitales: modelos virtuales de fábricas, edificios o ciudades alimentados por IoT.



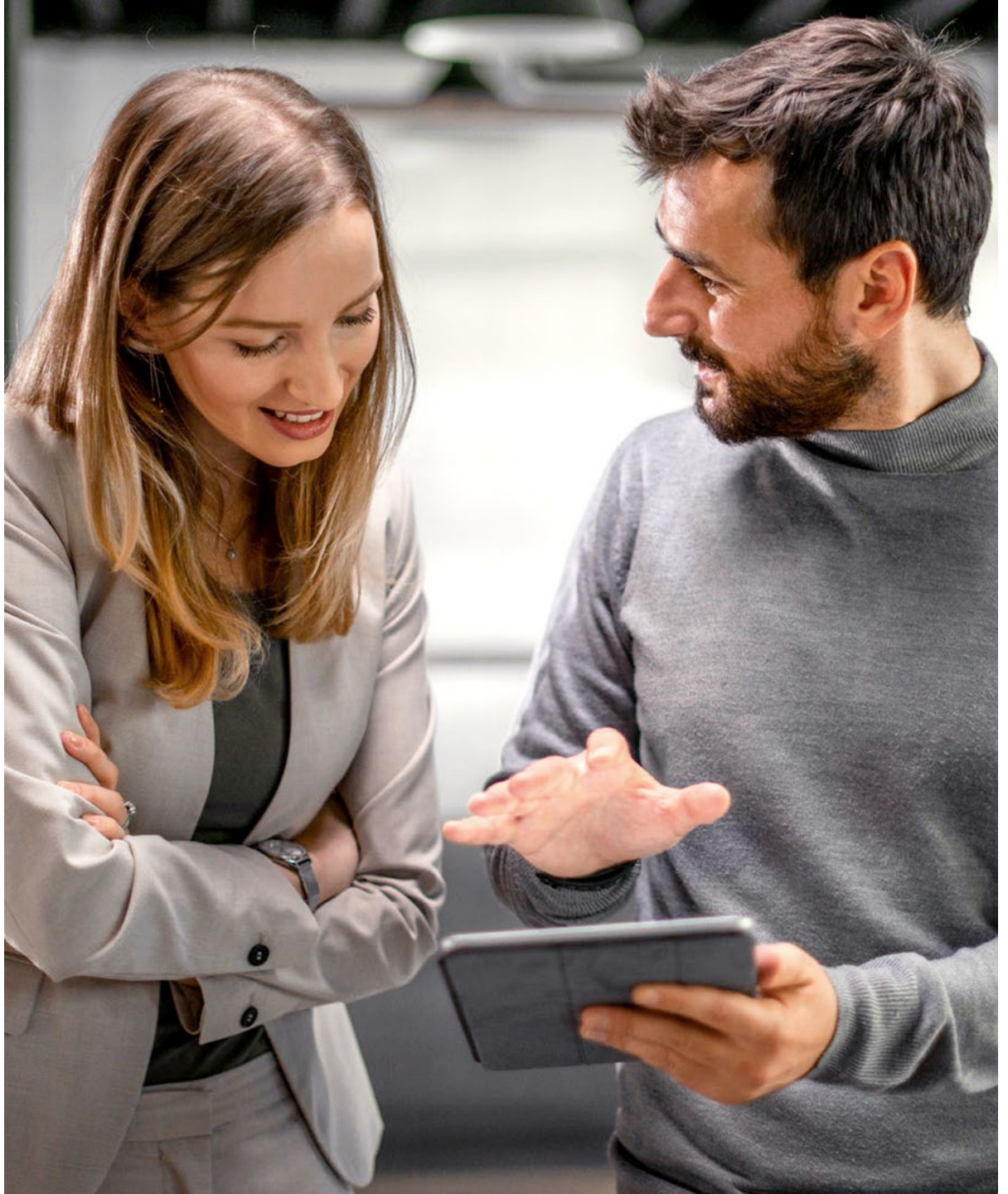
IoT deja de ser "sensores aislados" y se convierte en sistemas inteligentes distribuidos.

Internet of Things

Gestión de dispositivos IoT a escala

- **Inventario y visibilidad:** saber qué dispositivos están conectados, dónde y con qué configuración (muchos incidentes empiezan por dispositivos "olvidados").
- **Actualización de firmware y parches:** gestión remota y automatizada, con verificación de integridad y rollback en caso de fallo.
- **Segmentación de redes:** aislar dispositivos IoT del resto de la red corporativa para limitar movimientos laterales si un dispositivo se compromete.

Sin gestión centralizada, cada nuevo dispositivo IoT es un punto ciego potencial.



https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

Internet of Things

Gemelos digitales: del sensor al simulador

Un **gemelo digital** es una réplica virtual de un sistema físico (fábrica, edificio, ciudad) alimentada en tiempo real por datos IoT.

Permite simular escenarios, optimizar operaciones y detectar anomalías antes de que ocurran en el mundo real.

Aplicaciones: mantenimiento predictivo en industria, optimización energética en edificios inteligentes, planificación urbana en Smart Cities.

El gemelo digital convierte datos IoT en capacidad de anticipación y decisión.

Internet of Things

Retos de seguridad y privacidad en IoT

Más superficie de ataque: miles de dispositivos, muchos poco protegidos.

Gestión de identidades, firmware y actualizaciones a gran escala.

Datos sensibles (localización, salud, hábitos) que viajan y se almacenan en la nube.

Cada nuevo dispositivo conectado es un nuevo posible punto de fallo… o de entrada.

Internet of Things

Mini–actividad · Identificar riesgos en un caso de Smart City

- **Contexto:** Una ciudad de tamaño medio despliega IoT para gestionar semáforos, alumbrado público, sensores de calidad del aire y cámaras de tráfico conectadas.
- **Trabajo en parejas (5–7 minutos):**
  - Identificad **2 riesgos de seguridad** principales (acceso no autorizado, manipulación de datos, disponibilidad…).
  - Proponed **1 medida técnica** y **1 medida organizativa** para mitigarlos.

No buscamos la solución perfecta, sino pensar en términos de impacto y mitigación.

07

Ciberseguridad en entornos digitales

Amenazas actuales, nuevos paradigmas y seguridad en la era de la IA

Ciberseguridad en entornos digitales

Panorama actual de amenazas

Ransomware como servicio, ataques a la cadena de suministro y APTs dirigidos a sectores críticos.

Más automatización y profesionalización del ciberdelito, con impacto en salud, energía, administración y banca.

Entornos híbridos: on-prem, cloud, SaaS, IoT y trabajo remoto amplían la superficie de ataque.

El objetivo ya no es "que no pase nada", sino detectar, contener y recuperarse más rápido.

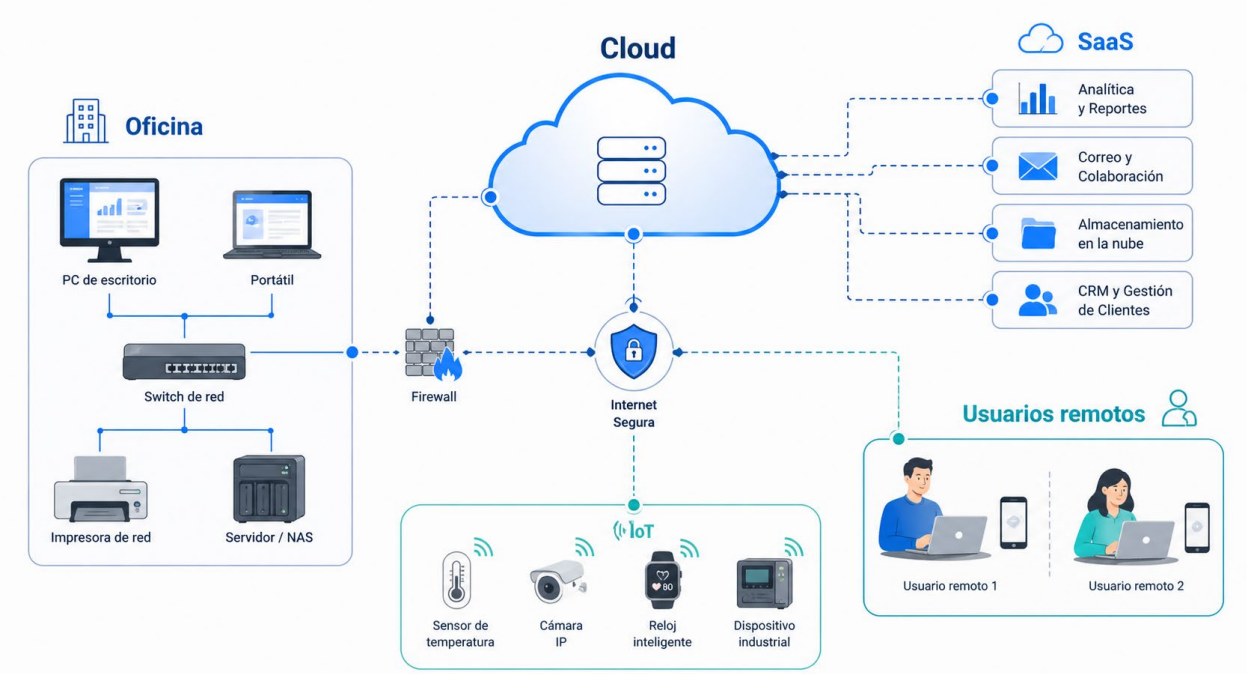
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Ciberseguridad en entornos digitales

Superficie de ataque en entornos híbridos y distribuidos

- Activos dispersos: usuarios, dispositivos, aplicaciones y datos repartidos entre redes internas, nubes públicas y SaaS.
- Nuevos vectores: credenciales robadas, APIs expuestas, dispositivos IoT inseguros, proveedores de terceros.
- Ataques laterales: el adversario entra por el eslabón más débil y se mueve internamente hasta los sistemas críticos.

La pregunta clave deja de ser "¿hay un firewall?" y pasa a ser "¿qué pasa cuando alguien ya está dentro?".



Ciberseguridad en entornos digitales

Principios básicos y marcos de referencia

- Triada **CIA**: confidencialidad, integridad, disponibilidad, extendida con autenticidad y trazabilidad.

Enfoque basado en riesgos, alineado con el **NIST Cybersecurity Framework** (Govern, Identify, Protect, Detect, Respond, Recover).

Estrategia de Ciberseguridad de la UE: resiliencia, capacidad operativa y cooperación, con ENISA como agencia clave de referencia.

Los principios son estables; lo que cambia son los entornos, las amenazas y las herramientas.

https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framewor

Nuevos paradigmas de defensa – Zero Trust y SASE

- Zero Trust: “never trust, always verify” → verificación continua de identidades, dispositivos, contexto y petición.
- SASE (Secure Access Service Edge): red y seguridad como servicio desde la nube, unificando acceso seguro a apps on-prem y cloud.
- Alineado con marcos como NIST CSF: controlar accesos, segmentar, monitorizar y responder de forma orquestada.

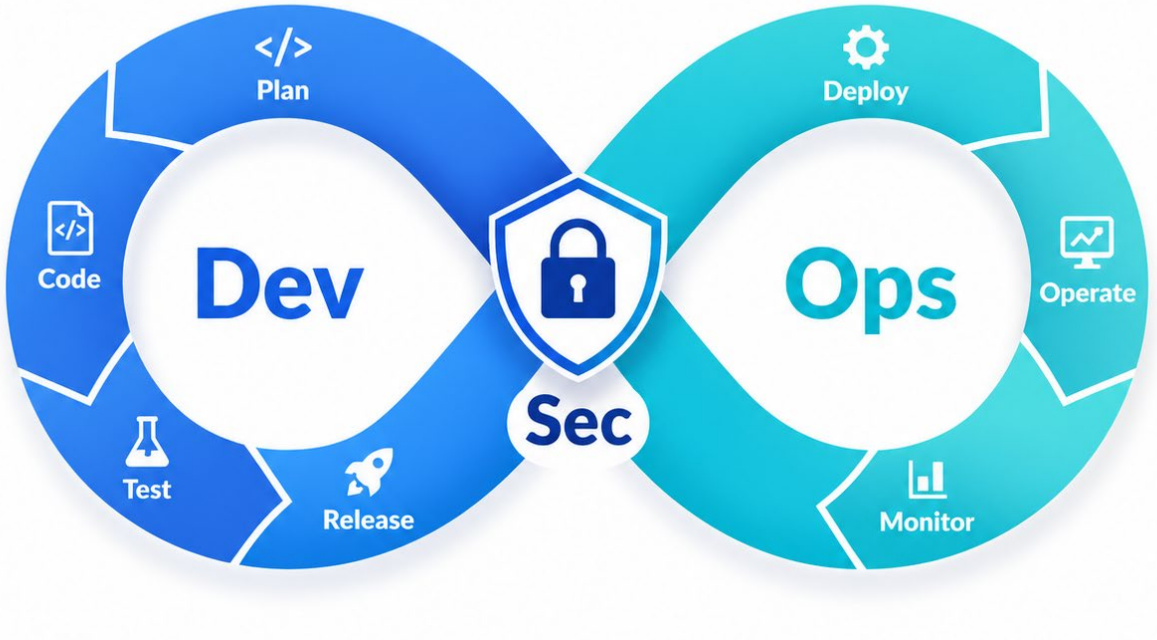
Zero Trust no es un producto, es una forma de pensar la arquitectura y el acceso.

https://www.cisco.com/site/us/en/learn/topics/security/what-is-secure-access-service-edge-sase.html

DevSecOps y seguridad por diseño

- Integrar seguridad en todo el ciclo de vida: threat modeling, SAST/DAST, análisis de dependencias, IaC scanning.
- “Shift-left”: detectar vulnerabilidades en código, pipelines y configuraciones antes de llegar a producción.
- Buenas prácticas alineadas con guías de NIST y ENISA: hardening, gestión de parches, revisión de terceros.

La seguridad eficaz se construye en el pipeline, no solo en el perímetro.



Ciberseguridad en entornos digitales

Seguridad en cloud, IoT y ecosistemas distribuidos

- Cloud: identidades y permisos, cifrado y gestión de claves, configuración segura de servicios gestionados.
- IoT: inventario de dispositivos, firmware seguro, actualización remota, segmentación de redes y guías como las de **ENISA** e **INCIBE**.
- Ecosistema UE: directiva NIS2 y recomendaciones de ENISA para gestión de cibercrisis y servicios esenciales.

Cuanto más distribuida es la arquitectura, más crítica es la visibilidad y el gobierno central de la seguridad.

Ciberseguridad en entornos digitales

La IA como arma de doble filo en ciberseguridad

- La IA ayuda a defender: detección de anomalías, priorización de alertas, respuesta más rápida ante incidentes.
- La IA también ayuda a atacar: phishing más convincente, malware generado o adaptado automáticamente, búsqueda de vulnerabilidades a escala.

La IA generativa amplifica tanto las capacidades defensivas como las ofensivas, reduciendo barreras de entrada para atacantes menos sofisticados.

La pregunta ya no es "IA sí o no", sino "cómo la usamos de forma responsable y segura".

IA ofensiva: ataques más rápidos y más creíbles

Deepfakes y generación de contenidos falsos para fraude, extorsión y operaciones de influencia.

- Phishing asistido por IA: mensajes mejor redactados, personalizados y masivos a bajo coste.
- Automatización del kill chain: reconocimiento, explotación y movimiento lateral apoyados en agentes autónomos e IA generativa.

La IA reduce la barrera de entrada para lanzar ataques sofisticados a gran escala.

IA defensiva: detección y respuesta aumentadas

Modelos de detección de anomalías en tráfico, logs y comportamiento de usuarios (UEBA, NDR, EDR “inteligentes”).

- SOC aumentado: priorización de alertas, correlación entre fuentes y soporte a analistas mediante asistentes basados en IA.
- Aplicación de marcos NIST/ENISA al ciclo Detect–Respond–Recover: IA como ayuda para reducir tiempo de detección y de contención.

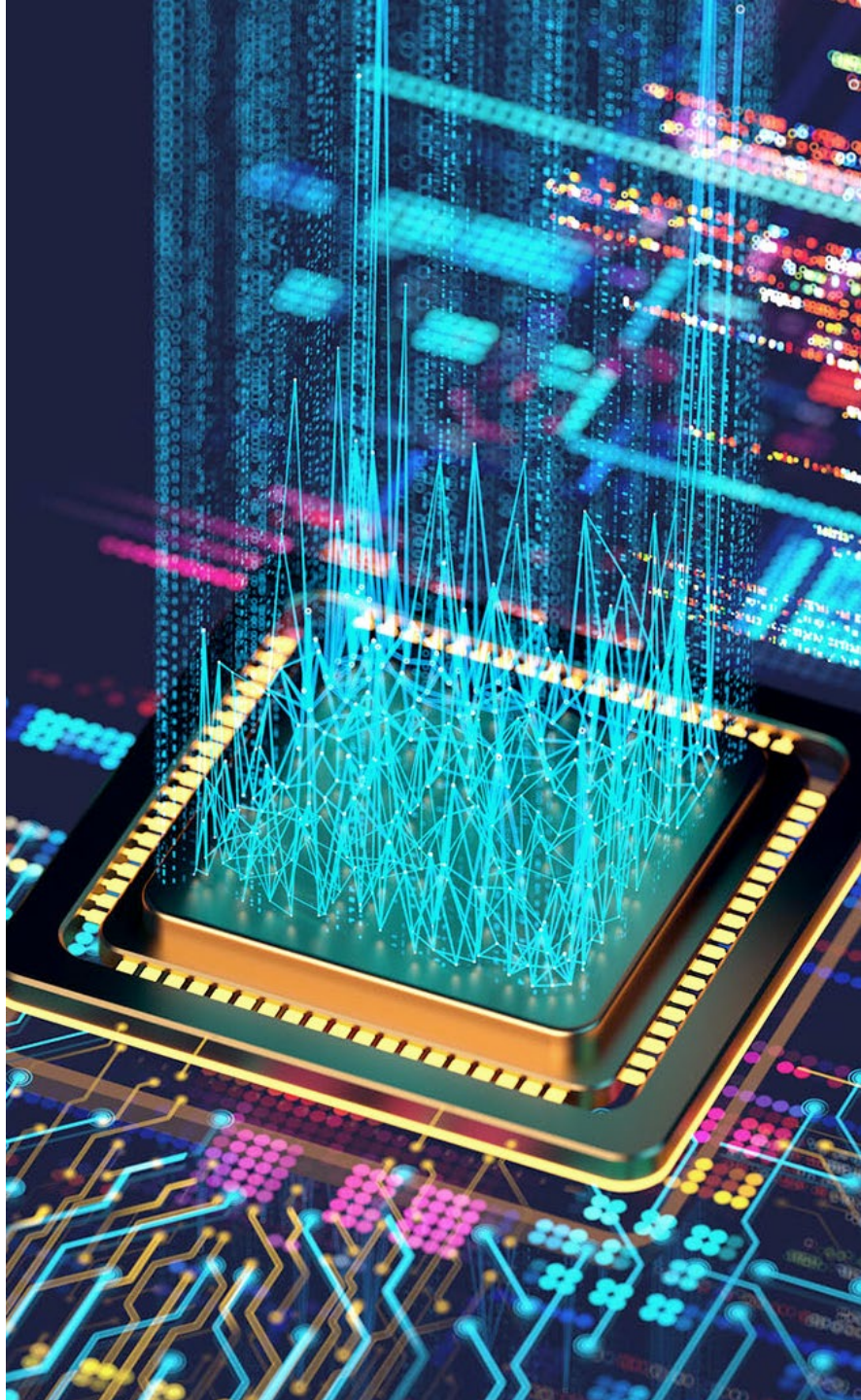
La IA defensiva no sustituye al analista: le libera de ruido para que se concentre en las decisiones.

Ciberseguridad en entornos digitales

Seguridad DE la IA: proteger modelos y datos

- Amenazas específicas: prompt injection, data exfiltration, model poisoning, backdoors y extracción de modelos.
- Riesgos de privacidad y cumplimiento (RGPD, AI Act): filtrado de datos personales y entrenamiento con datos sensibles sin control.
- Recomendaciones emergentes (NIST AI RMF, AI Act): evaluación de riesgos, pruebas adversariales, registro de interacciones, controles de acceso.

Los sistemas de IA se convierten en nuevos activos críticos que también hay que inventariar, proteger y auditar.



OWASP Top 10 para aplicaciones LLM y de IA generativa

OWASP ha publicado un **Top 10 específico para aplicaciones basadas en LLM y GenAI**, con los riesgos más críticos en este tipo de sistemas.

Incluye problemas como inyección de prompts, filtrado de información sensible, cadena de suministro insegura, envenenamiento de datos/modelos o manejo inadecuado de la salida.

La idea no es que memoricéis la lista, sino que veáis que ya hay un lenguaje común para hablar de seguridad en sistemas de IA generativa, igual que lo hubo para aplicaciones web.

Mismo patrón que con otras tecnologías: primero se generaliza el uso, luego la comunidad captura los riesgos recurrentes y propone mitigaciones.

OWASP Top 10 para aplicaciones LLM y de IA generativa

LLM01	LLM02	LLM03	LLM04	LLM05
Inyección de Prompts	**Manejo Inseguro de Salidas**	**Envenenamiento de Datos de Entrenamiento**	**Denegación de Servicio del Modelo**	**Vulnerabilidades en la Cadena de Suministro**
Manipula un modelo de lenguaje (LLM) a través de entradas ingeniosas, causando acciones no deseadas. Las inyecciones directas sobrescriben los prompts del sistema, mientras que las indirectas manipulan entradas de fuentes externas.	Esta vulnerabilidad ocurre cuando la salida de un LLM se acepta sin escrutinio, exponiendo sistemas backend. Su uso indebido puede tener consecuencias graves como XSS, CSRF, SSRF, escalada de privilegios o ejecución remota de código.	Se refiere a la manipulación de los datos o del proceso de ajuste fino (fine-tuning) para introducir vulnerabilidades, puertas traseras o sesgos que podrían comprometer la seguridad, eficacia o el comportamiento ético del modelo.	Los atacantes provocan operaciones con un alto consumo de recursos en los LLM, lo que provoca la degradación del servicio o costes elevados. La vulnerabilidad se magnifica debido a la naturaleza intensiva de recursos de los LLM.	El ciclo de vida de la aplicación LLM puede verse comprometido por componentes o servicios vulnerables, lo que conduce a ataques de seguridad. El uso de conjuntos de datos de terceros, modelos pre-entrenados y plugins añade vulnerabilidades.
LLM06	**LLM07**	**LLM08**	**LLM09**	**LLM10**
Divulgación de Información Sensible	**Diseño Inseguro de Plugins**	**Excesiva Autonomía (Excessive Agency)**	**Exceso de Confianza (Overreliance)**	**Robo de Modelos**
Los LLM pueden revelar inadvertidamente datos confidenciales en sus respuestas, lo que da lugar a accesos no autorizados, violaciones de privacidad y brechas de seguridad. Implemente la sanitización de datos para mitigar esto.	Los plugins de LLM pueden tener entradas inseguras y un control de acceso insuficiente. Los atacantes pueden explotar estas vulnerabilidades, resultando en consecuencias graves como la ejecución remota de código.	Los sistemas basados en LLM pueden realizar acciones que conduzcan a consecuencias no deseadas. El problema surge de la funcionalidad, los permisos o la autonomía excesiva otorgada a estos sistemas.	Los sistemas o personas que dependen excesivamente de los LLM sin supervisión pueden enfrentarse a desinformación, falta de comunicación, problemas legales y vulnerabilidades de seguridad debido a contenido incorrecto.	Implica el acceso no autorizado, copia o exfiltración de modelos de LLM propietarios. El impacto incluye pérdidas económicas, compromiso de la ventaja competitiva y acceso potencial a información sensible.

Fuente: https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-2023-slides-v1_0.pdf

Aprendizaje federado y datos sintéticos: nuevas piezas del puzzle

- Aprendizaje federado: entrenar modelos donde están los datos (endpoints, dispositivos, servidores) sin centralizarlos, mejorando detección distribuida y privacidad.

  Esto permite compartir solo parámetros del modelo para detectar malware y anomalías de forma colaborativa, alineándose mejor con marcos de privacidad (RGPD, etc.).

- Datos sintéticos: generar datos artificiales de alta calidad para pruebas y entrenamiento, reduciendo el uso de datos reales y riesgos de filtrado o re-identificación.

Las mismas técnicas que usamos para proteger datos (federated learning, datos sintéticos) añaden complejidad y abren nuevas preguntas sobre robustez y gobernanza.

Ciberseguridad en entornos digitales

Gobierno de IA segura (AI TRiSM, NIST, UE)

- Marcos de referencia: NIST Cybersecurity Framework 2.0 y NIST AI Risk Management Framework aplicados a sistemas de IA.
- Concepto de **AI TRiSM**: combinar confianza, riesgo y seguridad en IA (políticas de uso, gestión de terceros, explicabilidad, monitorización).
- Papel de la UE: AI Act europeo, Estrategia de Ciberseguridad y rol de ENISA como fuente de guías y buenas prácticas.

Gobernar IA segura es conectar marcos técnicos (NIST), buenas prácticas europeas (ENISA) y las obligaciones regulatorias (AI Act, NIS2).

Ciberseguridad en entornos digitales

Caso de estudio – Incidente de ciberseguridad en un entorno híbrido

Empresa europea de tamaño medio que presta servicios digitales a ayuntamientos (portal web de ciudadanía, app móvil y herramientas internas).

- Entorno híbrido: CPD on-premises, servicios en la nube pública (IaaS/PaaS) y varias aplicaciones SaaS; pilotos de IoT en edificios inteligentes.

  La empresa entra en el ámbito de **NIS2** como entidad importante, con obligaciones reforzadas de gestión de riesgos y notificación de incidentes.

- *Frames de referencia: NIST Cybersecurity Framework, guías de ENISA y Directiva NIS2.*

Caso de estudio – Señales del incidente y tareas

¿Qué hacemos en las primeras 24 horas?

Lunes por la mañana se detectan anomalías:

- Múltiples intentos (algunos exitosos) de acceso administrador desde IPs extranjeras y fuera de horario.
- Picos de tráfico saliente desde varios servidores on-prem y una suscripción cloud.
- Lentitud y caídas intermitentes en aplicaciones internas y en el portal de ciudadanía; algunos backups del fin de semana han fallado.

Trabajo en grupos (10–12 minutos)

¿Qué tipo(s) de ataque creéis que podrían estar ocurriendo (compromiso de credenciales, movimiento lateral, exfiltración, ransomware…)?

Usando las funciones del **NIST CSF** (Govern–Identify–Protect–Detect–Respond–Recover), anotad 2–3 acciones prioritarias para las primeras 24 horas.

¿En qué momento y cómo entrarían en juego las obligaciones de **NIS2** y las buenas prácticas de **ENISA** en gestión de incidentes (detección, notificación, coordinación, lecciones aprendidas)?

No buscamos la respuesta perfecta, sino practicar cómo estructurar decisiones bajo presión usando marcos reconocidos.

08

Computación cuántica y tendencias emergentes

¿Qué viene después y qué implica para la ciberseguridad?

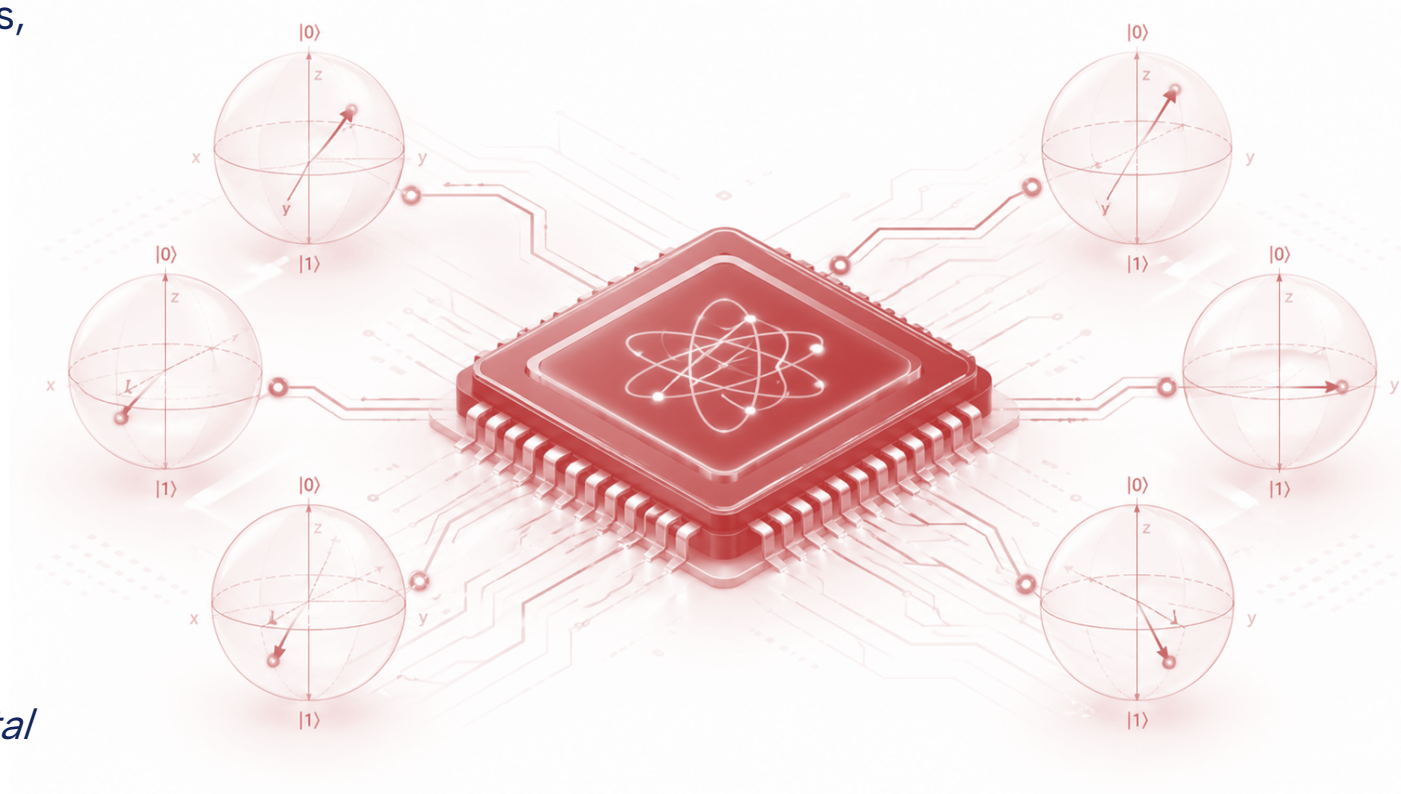
¿Qué es la computación cuántica?

Ordenadores que usan **qubits** en lugar de bits, aprovechando fenómenos como la superposición y el entrelazamiento.

No son “PCs más rápidos” para todo, sino máquinas diseñadas para resolver ciertos problemas mucho más rápida que los ordenadores clásicos.

Estamos aún en una fase temprana (equipos ruidosos, pocos qubits útiles), pero los avances marcan el ritmo de la conversación sobre criptografía y seguridad a largo plazo.

La computación cuántica es más un cambio de modelo que una simple mejora incremental de rendimiento.



Computación cuántica y tendencias emergentes

Impacto en criptografía: amenaza y oportunidad

Algoritmos como **Shor** muestran que, con ordenadores cuánticos suficientemente potentes, buena parte de la criptografía de clave pública actual (RSA, ECC) dejaría de ser computacionalmente segura.

Esto abre la puerta a escenarios de “harvest now, decrypt later”: datos cifrados hoy podrían descifrarse en el futuro si se guardan durante años.

A la vez, la comunidad está definiendo y estandarizando **criptografía post-cuántica (PQC)** resistente a ataques cuánticos (iniciativas de NIST y organismos europeos).

El reto no es solo técnico, sino de tiempos: qué datos queremos sigan siendo confidenciales dentro de 10–20 años.

https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved

Computación cuántica y tendencias emergentes

Criptografía post-cuántica y transición

Nuevos esquemas criptográficos diseñados para resistir ataques cuánticos, ya en proceso de estandarización.

- Retos prácticos: rendimiento, tamaños de claves y firmas, compatibilidad con protocolos y sistemas existentes, y coexistencia con algoritmos clásicos.
- La transición debe planificarse: plan de migración, "cripto-agilidad" y alineación con estrategias nacionales/europeas

No se trata solo de cambiar algoritmos, sino de preparar organizaciones y sistemas para varios años de convivencia híbrida.

https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved

Computación cuántica y tendencias emergentes

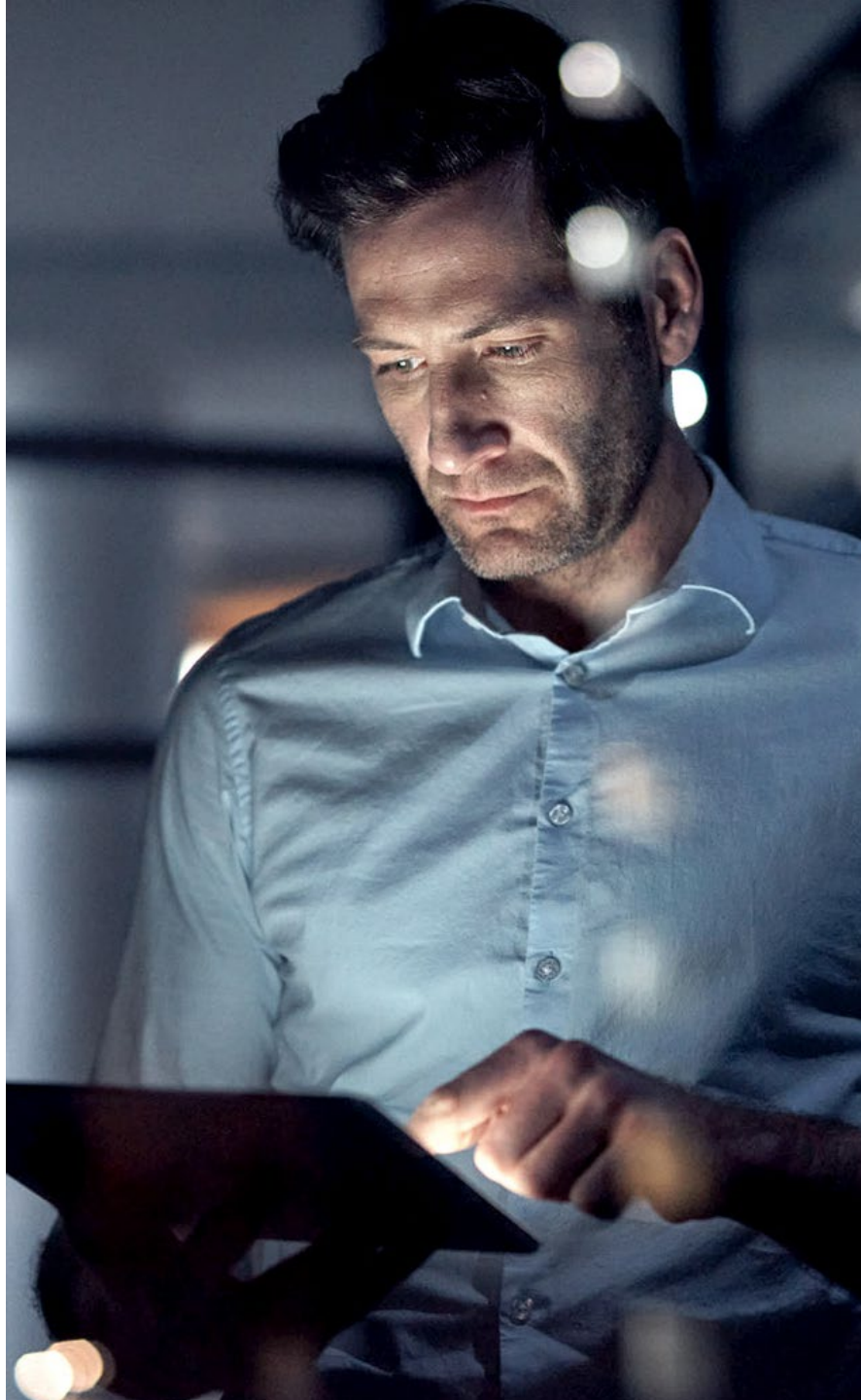
Más allá del cripto: ¿para qué podría servir?

Optimización y simulación a gran escala: logística, energía, química, materiales… con impactos indirectos sobre cómo diseñamos redes, defensas y sistemas críticos.

Exploración en **machine learning cuántico (QML)** y seguridad post-cuántica aplicada a entornos industriales (proyectos que combinan PQC, QKD e IA).

Mucho ruido de marketing, pero conviene entender el mapa para separar hype de oportunidades reales y prepararse para hablar con criterio.

La computación cuántica no va a sustituir a la clásica, pero sí puede cambiar cómo abordamos ciertos problemas difíciles.



Computación cuántica y tendencias emergentes

Tendencias en automatización y defensa

Más **automatización en detección y respuesta**: XDR, SOAR e IA defensiva para reducir tiempos de detección y contención.

Identidad como nuevo perímetro: MFA robusta, gestión de accesos privilegiados, segmentación basada en identidad y comportamiento.

Marcos y guías (NIST CSF, Essential Eight, etc.) como forma de priorizar controles en lugar de perseguir “la herramienta de moda”.

Sin una estrategia clara, más herramientas no implican más seguridad, sino más complejidad.

Computación cuántica y tendencias emergentes

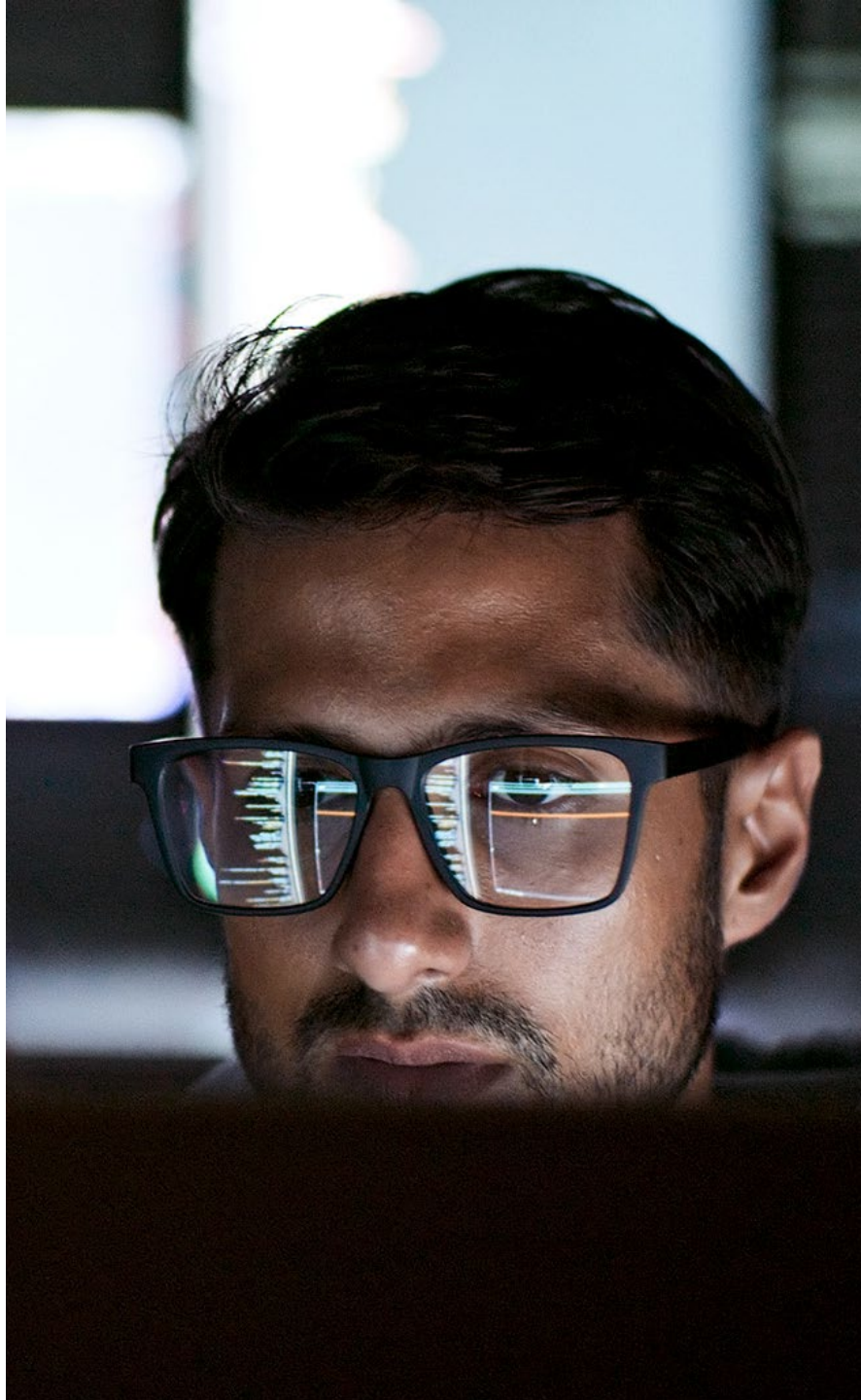
El factor humano en ciberseguridad

La mayoría de los incidentes de seguridad tienen algún componente humano: clics en enlaces, uso de contraseñas débiles, errores de configuración, decisiones de negocio que ignoran riesgos.

Los atacantes explotan esa realidad con ingeniería social, phishing dirigido, deepfakes y otros mecanismos que apuntan a personas y equipos, más que a fallos puramente técnicos.

Una estrategia sólida combina tecnología con **procesos, formación, cultura y liderazgo**: sin eso, cualquier herramienta se queda corta.

No hablamos solo de "parches y firewalls", sino de cómo trabajamos, decidimos y aprendemos como organización.



Computación cuántica y tendencias emergentes

Computación cuántica y tendencias emergentes

Otras tendencias a vigilar

Soberanía digital: iniciativas europeas sobre datos, cloud y ciberseguridad, y su impacto en dónde y cómo desplegamos servicios.

Regulación creciente (NIS2, AI Act, privacidad) que exige perfiles híbridos capaces de traducir requisitos legales a decisiones técnicas.

Seguridad en entornos OT/IIoT críticos (energía, agua, transporte, manufactura): convergencia IT/OT y necesidad de enfoques específicos.

Computación cuántica y tendencias emergentes

Actividad final – Radar personal de tendencias

Trabajo individual o en parejas (8–10 minutos).

Elegid **una tendencia** del módulo que creáis especialmente relevante para vuestro contexto profesional o formativo: cloud, IoT, IA en ciberseguridad, PQC, soberanía digital, automatización, etc.

Responded de forma breve a estas preguntas:

- **¿Qué tendencia tiene más impacto potencial en mi contexto?**
- **¿Qué problema podría resolver?**
- **¿Qué riesgo introduce?**
- **¿Qué barrera de adopción tendría?**
- **¿Qué primer paso razonable podría darse?**

Computación cuántica y tendencias emergentes

¿Qué nos llevamos de esta parte del módulo?

Cloud y datos (unidad 5)

Entender arquitecturas y modelos de servicio para tomar decisiones informadas, no por moda.

IoT (unidad 6)

Pensar en sistemas completos, no en dispositivos aislados; importancia de edge, conectividad y gobierno del dato.

Ciberseguridad (unidad 7)

Hablar en términos de marcos (NIST, ENISA, NIS2, OWASP) y gestión de riesgos, no solo de productos.

Tendencias (unidad 8)

Horizonte cuántico, automatización e IA, factor humano y regulación como ejes para los próximos años.

¡Gracias!

GENERACIÓN D
UNIÓN PROFESIONAL
Upro
Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia