

Criptoinventario y Criptoagilidad

El nuevo estándar de seguridad postcuántica

¿Qué es el Criptoinventario?

El **criptoinventario** permite **identificar, unificar y mapear** todos los **mecanismos criptográficos** de la organización, **algoritmos, certificados, librerías y sistemas** donde se utilizan. Además es la base que nos permitirá hacer un análisis de riesgo de la postura de **seguridad criptográfica** de la empresa u organismo, aportando visibilidad estructurada de la **huella criptográfica** y constituyendo el punto de partida imprescindible para cualquier **transición poscuántica**.

Ventajas de contar con Criptoinventario	Inconvenientes de no tener Criptoinventario
Visibilidad completa del entorno criptográfico	Desconocimiento de activos y dependencias críticas
Identificación temprana de algoritmos débiles u obsoletos	Presencia de algoritmos obsoletos sin detectar
Priorización de migraciones basada en riesgo real	Migraciones improvisadas y mayor riesgo operativo
Reducción del impacto operativo en procesos de actualización	Exposición a escenarios como Harvest Now, Decrypt Later
Mayor alineación con requisitos regulatorios y auditorías	Dificultad para cumplir exigencias normativas

¿Qué es la Criptoagilidad?

La **Criptoagilidad** es la capacidad de una organización para **gestionar, actualizar, sustituir o eliminar sus mecanismos criptográficos de forma rápida y controlada**, sin interrumpir la operación. Es una **capacidad estratégica de resiliencia digital** que permite adaptar la arquitectura **criptográfica** de forma **dinámica y gobernada**. En un entorno de amenazas emergentes, avances constantes en tecnologías como la computación cuántica o la inteligencia artificial y una **presión regulatoria creciente**, permite que la **seguridad** evolucione al ritmo del negocio sin convertirse en un freno tecnológico.

¿Qué permite?



Adaptación ágil ante nuevas vulnerabilidades o requisitos normativos



Transición híbrida entre criptografía tradicional y poscuántica (PQC)



Migración progresiva hacia criptografía poscuántica sin rediseños masivos



Menor riesgo en infraestructuras rígidas y mayor resiliencia a largo plazo

Nuestra propuesta de valor

Telefónica Tech ofrece una aproximación integral que combina **metodología, tecnología y gobernanza** para convertir la transición poscuántica en un proceso estructurado, medible y alineado con negocio.

Nuestra propuesta se articula en tres pilares:



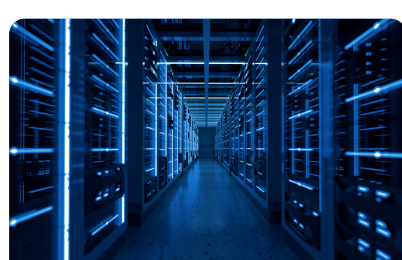
Identificación

Descubrimiento automatizado en red, código, APIs, contenedores y entornos cloud para generar un Crypto Bill of Materials (CBOM) completo, contextualizado por criticidad y riesgo.



Protección

Implementamos protección postcuántica sin interrupción, desacoplando aplicaciones de algoritmos y asegurando continuidad operativa ante la evolución criptográfica.



Gobernanza

Integramos la gestión criptográfica en el modelo corporativo de riesgo y cumplimiento, garantizando trazabilidad, alineación normativa y preparación futura.

¿Por qué somos tu socio ideal?

- **Acompañamiento integral** desde la visibilidad criptográfica inicial hasta la implantación efectiva de arquitecturas **Quantum Safe**, garantizando continuidad operativa.
- Experiencia probada en **sectores críticos y altamente regulados**, donde la **criptografía** es un pilar de **continuidad, cumplimiento y confianza digital**.

- **Ecosistema tecnológico** y alianzas estratégicas que integran inventario, **protección y gobernanza** en una **plataforma unificada**, acelerando la transición **postcuántica** con control y soberanía.
- Modelo operativo de **criptoagilidad** que transforma la migración **criptográfica** en una capacidad estructural y permanente de la **organización**.