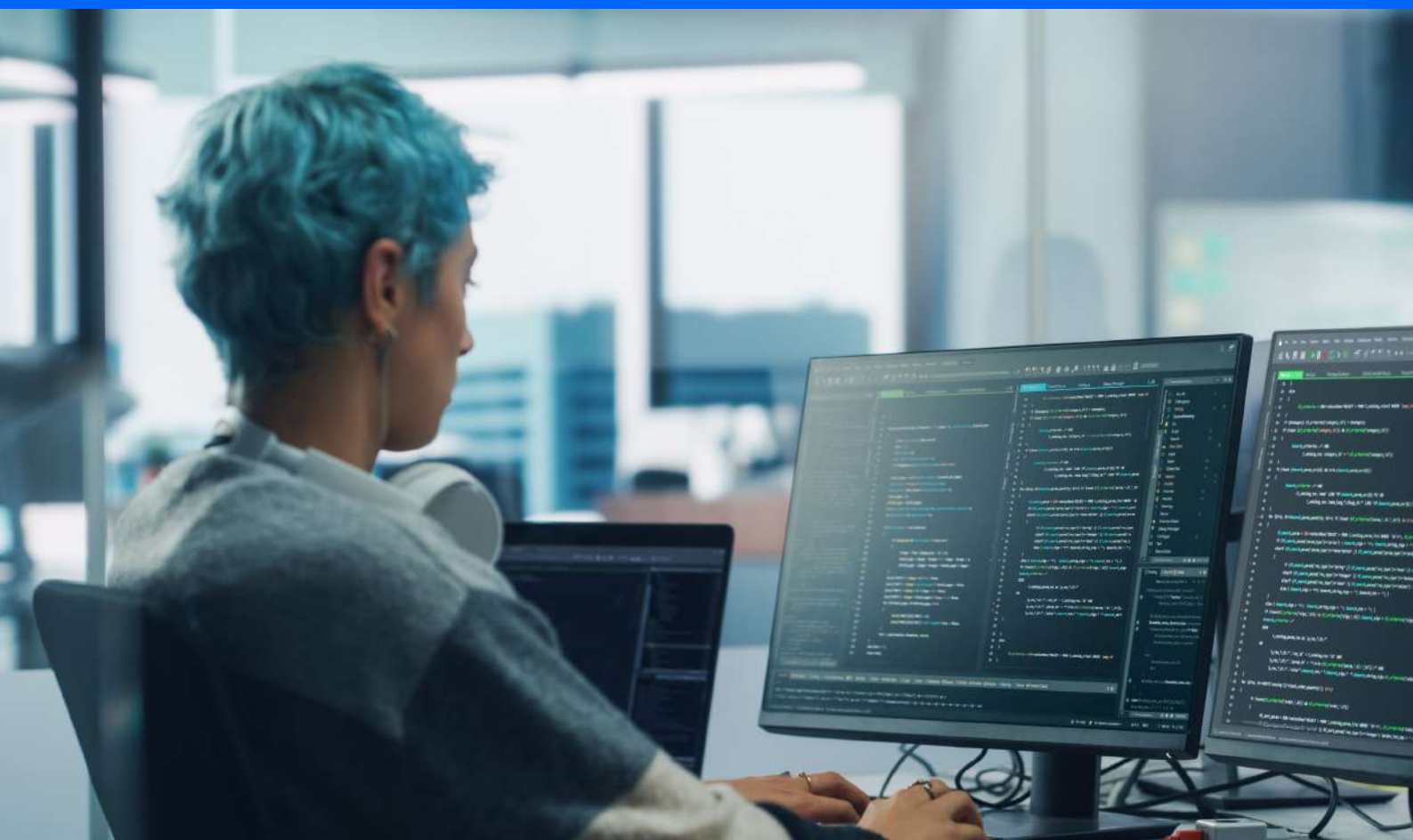
Telefónica Tech

Preparación estratégica para la Criptografía Poscuántica

La amenaza de la computación cuántica, la implementación de la criptografía poscuántica (PQC) y estrategias para una transición segura y eficaz.



Índice

Resumen 3

Introducción 4

El papel de la criptografía en la protección de los datos y la soberanía digital en la era poscuántica 5

Impacto en la criptografía actual 5
Algoritmos cuánticos clave: Shor y Grover 6

La amenaza del ataque cuántico: evaluación del impacto y preparación estratégica 6

Qué es la computación cuántica 6
Implicaciones operativas para las empresas 8
Implicaciones estratégicas y soberanía empresarial frente a la computación cuántica 9

Criptografía poscuántica (PQC) como respuesta técnica y estratégica 10

PQC para preservar la seguridad a largo plazo 10
Estandarización de NIST y otras entidades 10
Algoritmos seleccionados para la estandarización 11
Importancia de la estandarización 11
Papel de la UE y participación internacional 11

Pilares para una transición proactiva y gradual 12

Pilar 1. Identificar: Inventario criptográfico y evaluación de riesgos 13
Pilar 2. Proteger: Implementación de soluciones y transición segura 16
Pilar 3. Gobernar: Implementación y seguimiento continuo 20

Casos de uso sectoriales 23

Conclusiones y recomendaciones para asegurar el futuro digital en la era cuántica 25

Resumen

La criptografía es esencial para la seguridad y soberanía digital. Sin embargo, con la computación cuántica, los sistemas criptográficos asimétricos actuales serán vulnerables. Esto exige una transición hacia la criptografía poscuántica (PQC).

Este documento expone los riesgos, estrategias de transición y acciones recomendadas para proteger la información en la era cuántica.

Introducción

La soberanía digital es fundamental para asegurar la independencia y control de infraestructuras y datos. Este principio abarca dimensiones operativas, tecnológicas y de gestión de datos, y constituye la base de la autonomía de organizaciones y estados.

La criptografía es la base tecnológica de la soberanía que proporciona ese control y autonomía. Asegura la confidencialidad, integridad y disponibilidad de los datos, fundamentales para el funcionamiento de empresas, gobiernos y sociedades.

Sin embargo, este paradigma de seguridad enfrenta un cambio significativo con el avance de la computación cuántica. El momento Q-Day, cuando los ordenadores cuánticos puedan comprometer los sistemas actuales, podría llegar en 10 a 20 años, incluso antes. Aunque no hay un consenso exacto, y esta proyección depende del progreso en la computación cuántica y la escalabilidad de los qubits, esto exige preparación para garantizar la seguridad de los datos y las redes de comunicación.

La criptografía poscuántica (PQC) surge como respuesta técnica. Desarrolla algoritmos de cifrados resistentes a ataques de computadoras clásicas y cuánticas, basados en problemas matemáticos que los ordenadores cuánticos no pueden resolver de manera eficiente. Esto proporciona un nivel de seguridad adaptado a la era cuántica. La adopción de la criptografía poscuántica trasciende lo técnico. Es una decisión estratégica con implicaciones en la soberanía de las infraestructuras digitales. Al implementar PQC, organizaciones, empresas y gobiernos aseguran que sus datos e infraestructuras estén protegidos contra amenazas presentes y futuras.
De este modo, reafirman su capacidad de operar de manera independiente, manteniendo el control sobre sus activos digitales y preservando su soberanía.

¿Cuáles serían las consecuencias si alguien intercepta y almacena los datos más sensibles de tu empresa y los descifrara en 2030?

Este documento presenta una llamada a la acción para organizaciones, empresas y organismos nacionales. Es imperativo prepararse ahora para la transición a PQC.

Retrasar esta acción podría tener consecuencias significativas, incluyendo la exposición de datos sensibles, la interrupción de operaciones y el incumplimiento normativo.

La criptografía poscuántica **es implementable en hardware y software convencional.** Esto permite iniciar la transición hoy para asegurar la resiliencia y fiabilidad de la infraestructura digital en el futuro.

El papel de la criptografía en la protección de los datos y la soberanía digital en la era poscuántica

La encriptación protege los datos de accesos no autorizados y asegura la soberanía digital en almacenamiento, comunicaciones y nube. Impide vigilancia o interferencia externa, resguardando las comunicaciones de gobiernos, organizaciones o actores maliciosos.

Regulaciones como RGPD en Europa exigen el cifrado para asegurar la privacidad del usuario y la protección de datos personales. Además, la encriptación protege infraestructuras esenciales como telecomunicaciones, energía y servicios financieros, salvaguardando datos operativos y sistemas de control.

Es imprescindible prepararse ahora y migrar a nuevos algoritmos criptográficos cuánticos para preserver la protección de los datos y la soberanía digital a largo plazo.

Impacto en la criptografía actual

Desde el punto de vista de la ciberseguridad, el impacto potencial más significativo de la computación cuántica es su capacidad para comprometer la seguridad de muchos algoritmos criptográficos asimétricos (de clave pública) utilizados hoy.

- **Algoritmos en riesgo:** RSA, DSA, ECDSA y otros basados en la dificultad de la factorización de números enteros grandes o el problema del logaritmo discreto son vulnerables ante un ataque de una computadora cuántica criptográficamente relevante. Estos algoritmos son la base de la seguridad de protocolos como TLS / SSL (utilizado en HTTPS), SSH, firmas digitales y muchas infraestructuras de clave pública (PKI).

- **Criptografía simétrica (AES, SHA-256):** Aunque la computación cuántica afecta a la criptografía simétrica a través de algoritmos como el de Grover, el impacto es menos severo. Se requeriría un aumento en el tamaño de las claves para mantener un nivel de seguridad equivalente. Por ejemplo, AES-256 ofrece 128 bits de seguridad frente a ataques cuánticos (según el algoritmo de Grover), lo que equivale a la seguridad clásica de AES-128. En ataques cuánticos, AES requiere un incremento en la longitud de las claves para conservar su nivel de seguridad.

La amenaza de la estrategia 'Harvest now, decrypt later'

Los actores maliciosos han adoptado la estrategia de ataque Harvest Now, Decrypt Later (HNDL), o 'Store Now, Decrypt Later 'o 'Almacenar ahora, descifrar después', como una táctica a largo plazo.

HNDL consiste en la recolección masiva de datos cifrados mediante técnicas tradicionales para almacenarlos y descifrar con ordenadores cuánticos criptográficamente relevantes. Esto afecta a información con un largo periodo de confidencialidad, como secretos gubernamentales, propiedad intelectual o registros médicos, entre otros.

Se han identificado ataques HNDL de recolección masiva de datos cifrados de grupos APT (Amenazas Persistentes Avanzadas) vinculados a estados-nación, incluyendo interceptación de comunicaciones explotando vulnerabilidades en redes VPN o canales TLS, exfiltración de almacenamientos cloud con información cifrada, o redireccionamiento de tráfico.

Algoritmos cuánticos clave: Shor y Grover

- **Algoritmo de Shor:** Este algoritmo, desarrollado por Peter Shor, es la principal amenaza para la criptografía asimétrica actual. Permite factorizar números enteros grandes en tiempo polinómico, un avance significativo con respecto a los mejores algoritmos clásicos. Esto invalida la seguridad de RSA y algoritmos similares, y significa que los datos cifrados hoy con estos esquemas podrían ser descifrados en el futuro.

- **Algoritmo de Grover:** El algoritmo de Lov Grover reduce exponencialmente la complejidad de búsqueda a raíz cuadrada, lo que implica que AES-128 proporcionaría únicamente 64 bits de seguridad frente a ataques cuánticos. Para mantener la seguridad se recomienda, al menos, claves de 256 bits.

La amenaza del ataque cuántico: evaluación del impacto y preparación estratégica

Qué es la computación cuántica

La computación cuántica representa un paradigma computacional diferente al de la computación clásica. En lugar de bits, que representan un 0 o un 1, utiliza qubits. Utilizando principios de la mecánica cuántica como la superposición y el entrelazamiento, los qubits pueden representar 0, 1 o una combinación de ambos.

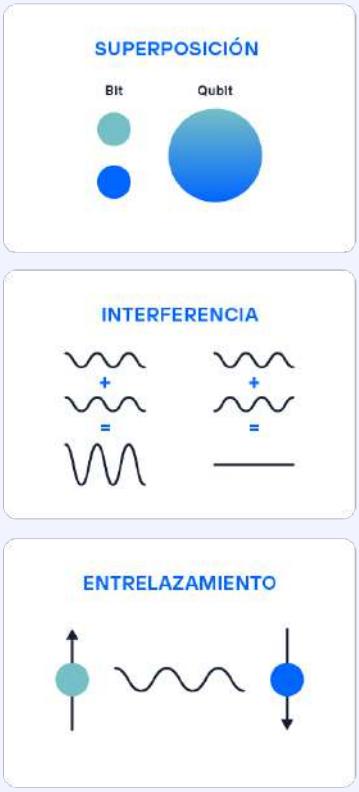
Esta capacidad permite a las computadoras cuánticas procesar un volumen de información exponencialmente mayor que las clásicas para ciertos problemas matemáticos.

La computación cuántica no es universalmente superior a la clásica. Su ventaja reside en su capacidad para abordar de manera eficiente problemas de gran complejidad matemática en dominios como la simulación molecular, la optimización combinatoria y, de particular relevancia para este documento, la criptografía.

El Instituto Nacional de Estándares y Tecnología (NIST) recomienda eliminar RSA-2048 y ECC-256 antes de 2030, con su completa invalidación para 2035. Como parte de la transición a la criptografía poscuántica, el NIST insta a las organizaciones a migrar a algoritmos resistentes a la computación cuántica antes de esas fechas.

Imagina un laberinto gigante donde la salida representa la solución a un problema complejo, como descifrar un código criptográfico.

Un ordenador clásico intentaría resolver el laberinto probando cada camino uno por uno, lo que podría tardar años si hay millones de combinaciones posibles.



En cambio, un ordenador cuántico, gracias al principio de **superposición**, puede explorar múltiples caminos en paralelo. Además, el **entrelazamiento cuántico** permite correlacionar los resultados de diferentes estados cuánticos, lo que facilita encontrar la solución correcta con mayor eficiencia en ciertos tipos de problemas.

Esto significa que, en casos específicos como la **factorización de enteros grandes** (clave en RSA) o el **cálculo del logaritmo discreto** (usado en DSA, ECDSA), un ordenador cuántico ejecutando el **algoritmo de Shor** podría resolverlos mucho más rápido que cualquier método clásico conocido.

Sin embargo, no todos los cifrados son vulnerables. Algoritmos basados en **criptografía poscuántica** han sido diseñados para resistir estos ataques, incluso frente a ordenadores cuánticos.

Aunque los ordenadores cuánticos no pueden romper todos los cifrados ni resolver todos los problemas más rápido, su capacidad de paralelismo cuántico **plantea un desafío profundo a la seguridad digital actual**, especialmente para la criptografía asimétrica.

Implicaciones operativas para las empresas

La amenaza cuántica presenta un riesgo estratégico y operativo significativo para cualquier organización, entidad o empresa que dependa de la criptografía para proteger sus datos y comunicaciones.
Algunas de las consecuencias incluyen:

Riesgos y vulnerabilidades

- **Riesgo de exposición de datos:** La información cifrada con algoritmos vulnerables a computación cuántica podría ser descifrada en el futuro, comprometiendo datos sensibles, secretos comerciales, propiedad intelectual y comunicaciones confidenciales.
  Esto es crítico para datos con largo ciclo de vida.

- **Protección contra injerencias externas:** El cifrado robusto es fundamental para mantener la soberanía sobre los datos almacenados y en tránsito, especialmente en entornos cloud. El cifrado protege contra la vigilancia y el acceso no autorizado de gobiernos, organizaciones o ciberdelincuentes.

Desafíos operativos y estratégicos

- **Interrupción operativa:** Reemplazar los sistemas criptográficos actuales representa un desafío operativo. La migración a la criptografía poscuántica requerirá planificación, inversión y gestión cuidadosa para evitar interrupciones en los servicios.

- **Coste de la inacción:** Retrasar la preparación para la criptografía poscuántica podría resultar en costes mayores en el futuro, tanto en remediación de vulnerabilidades como en posibles pérdidas por brechas de seguridad.

Oportunidades y responsabilidades

- **Ventaja competitiva:** Las organizaciones que adopten proactivamente la criptografía poscuántica pueden obtener una ventaja competitiva al ofrecer mayor seguridad y demostrar su compromiso con la protección de los datos de sus clientes.

- **Cumplimiento normativo:** El cumplimiento de RGPD en Europa exige cifrado actual y adaptación a estándares poscuánticos para mantener la protección de datos personales a largo plazo.

Áreas clave de aplicación

- **Protección de infraestructuras críticas:** El cifrado poscuántico protege infraestructuras críticas como telecomunicaciones, energía y sistemas financieros, salvaguardando los datos operativos y sistemas de control.

- **Servicios digitales de confianza:** Las organizaciones pueden ofrecer servicios digitales seguros y respetuosos con la privacidad, combinando el cifrado poscuántico con algoritmos de IA, y reforzando su compromiso con la soberanía digital.

Implicaciones estratégicas y soberanía empresarial frente a la computación cuántica

En el contexto de la seguridad basada en algoritmos criptográficos, la computación cuántica presenta riesgos y desafíos que deben ser abordados de forma proactiva:

- **Los algoritmos criptográficos comunes se volverán vulnerables**, poniendo en riesgo toda la información protegida. Es esencial priorizar la transición hacia criptografía poscuántica (PQC), que protege los datos en la era cuántica.
- La **migración a PQC** requerirá inversiones en tecnologías, software, hardware y, fundamentalmente, en la **capacitación del personal** para garantizar una transición segura.
- La **computación cuántica** debe integrarse en el marco de **gestión de riesgos empresariales,** con evaluaciones periódicas para identificar vulnerabilidades y medir el progreso hacia la adopción de PQC.
- Las **recomendaciones regulatorias** actuales evolucionarán hacia **exigencias de criptografía resistente**, lo que demanda anticipación y preparación para mitigar los riesgos.
- La **criptoagilidad** será clave para adaptar los sistemas criptográficos frente a nuevas amenazas y vulnerabilidades futuras.
- Una sólida **gobernanza criptográfica**, con visibilidad completa de activos digitales, asegura el cumplimiento normativo y una implementación eficiente.

A nivel estratégico, la soberanía digital y tecnológica será fundamental para alcanzar los objetivos empresariales:

- **Soberanía operativa:** Necesaria para optimizar la eficiencia, garantizar la seguridad de comunicaciones, IoT, IA e infraestructuras en la nube.
- **Soberanía tecnológica:** Vital para la resiliencia e independencia de las infraestructuras digitales, así como para el cumplimiento normativo y la autonomía operativa.
- **Soberanía de la IA y los datos:** Protege intereses nacionales, seguridad y privacidad, evitando influencias externas y garantizando decisiones basadas en información confiable.

Las empresas deben prepararse internamente y evaluar a proveedores y terceras partes para garantizar que sus dependencias externas no comprometan la transición a PQC. Prepararse para el **Q-Day** (día en que la computación cuántica será plenamente funcional) reducirá significativamente **costes y riesgos** de remediación si se actúa con anticipación.

Criptografía poscuántica (PQC) como respuesta técnica y estratégica

La criptografía poscuántica **(PQC)** o resistente a la computación cuántica, comprende el desarrollo de algoritmos criptográficos diseñados para resistir ataques de ordenadores clásicos y cuánticos.

Sin embargo, la criptografía poscuántica no depende de ordenadores cuánticos. PQC utiliza algoritmos matemáticos clásicos en hardware convencional, mientras que la computación cuántica usa QKD para el intercambio de claves y QRNG para generar números aleatorios. Estos algoritmos se consideran resistentes a ataques de computadoras cuánticas.

PQC para preservar la seguridad a largo plazo

La PQC es importante porque se necesita proteger la información con un horizonte de confidencialidad a largo plazo. Es difícil predecir cuándo habrá una computadora cuántica criptográficamente relevante, capaz de romper la criptografía actual, pero el consenso entre expertos y la previsión del NIST es que la computación cuántica debilitará la criptografía asimétrica existente hacia finales de esta década.

La sustitución de la criptografía asimétrica por criptografía segura desde el punto de vista cuántico exige una acción proactiva. La migración a PQC debe ser una prioridad.

Debido a esto, la información cifrada hoy con algoritmos vulnerables podría ser descifrada en el futuro con consecuencias graves. Por tanto, la transición a PQC no es solo una cuestión técnica, sino una estrategia de gestión de riesgos a largo plazo.

Estandarización de NIST y otras entidades

La estandarización es clave para la adopción e interoperabilidad de la PQC. Desde 2016, el Instituto Nacional de Estándares y Tecnología (NIST) de EE UU ha liderado un proceso de evaluación y estandarización de algoritmos PQC.

Este proceso, estructurado en varias rondas, ha involucrado a la comunidad criptográfica global en el análisis y evaluación de docenas de propuestas. El NIST ha sido el principal impulsor en la identificación y estandarización de algoritmos PQC, a través de su Post-Quantum Cryptography Project.

Algoritmos seleccionados para la estandarización

En agosto de 2024, el NIST publicó los primeros algoritmos de criptografía poscuántica, iniciando la protección contra la computación cuántica. Estos algoritmos, elegidos por la comunidad criptográfica global para su estandarización, nos permiten iniciar ya la transición poscuántica:

- **CRYSTALS-Kyber (KEM):** Basado en estructuras reticulares y el problema Learning With Errors (LWE), para uso general de encapsulamiento de claves.
- **CRYSTALS-Dilithium (Firma Digital):** También basado en estructuras reticulares, para uso general de firma digital.
- **FALCON (Firma Digital):** específicamente optimizado para tamaños de firma reducidos en comparación con Dilithium.
- **SPHINCS+ (Firma Digital):** Como una opción de firma digital basada en hash, aunque con un tamaño de firma considerablemente mayor.

NIST ha publicado la selección de estos primeros algoritmos para estándares oficiales de criptografía resistente a la computación cuántica y está considerando la estandarización de algoritmos adicionales.

Importancia de la estandarización

La estandarización de los algoritmos PQC asegura que los algoritmos seleccionados han sido evaluados y facilita la integración de sistemas y aplicaciones, promoviendo su adopción global al proporcionar:

- **Confianza:** La comunidad criptográfica internacional ha evaluado los algoritmos seleccionados.
- **Interoperabilidad:** La estandarización permite la interoperabilidad entre diferentes sistemas y aplicaciones.
- **Guía para la adopción:** Proporciona una hoja de ruta clara para organizaciones que buscan migrar a PQC, permitiéndoles seleccionar algoritmos con confianza.

Papel de la UE y participación internacional

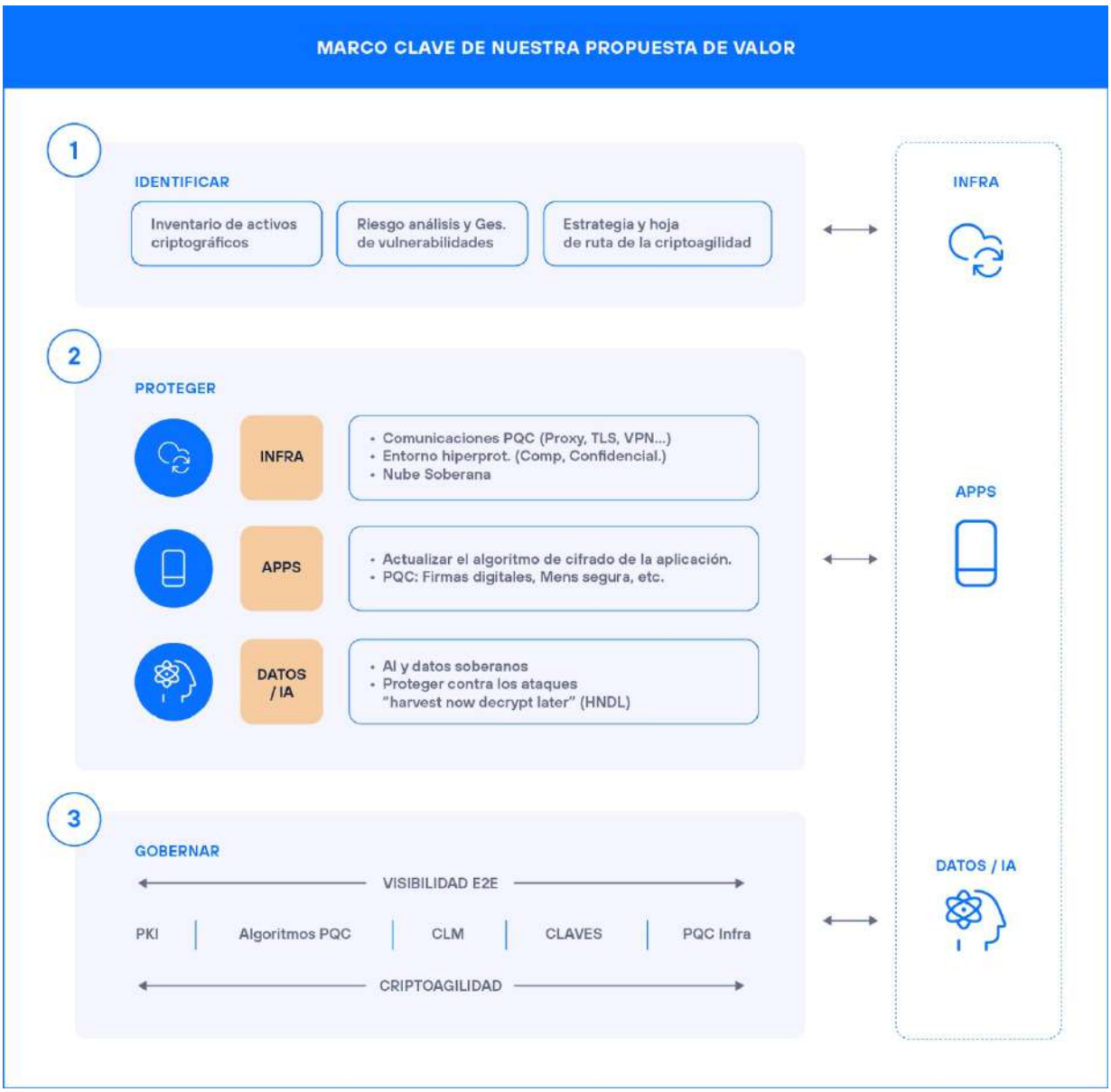
Otras organizaciones, como ISO y ETSI, también están involucradas en la estandarización de la PQC, asegurando una adopción global y coordinada. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) también juega un papel importante, proporcionando orientación y recomendaciones sobre la transición a PQC en el contexto europeo.

ENISA trabaja con el NIST y otras organizaciones internacionales para promover la adopción de estándares globales y mejores prácticas en criptografía poscuántica. Ha publicado informes y recomendaciones sobre PQC, incluyendo evaluaciones de la madurez de los algoritmos y guías para la migración.

La estandarización de algoritmos de criptografía resistente a la computación cuántica del NIST marca el inicio de la transición a PQC. La investigación en criptografía poscuántica continúa y es probable que se desarrollen y estandaricen nuevos algoritmos.

Pilares para una transición proactiva y gradual

La transición a la criptografía poscuántica es un proceso complejo que debe abordarse de manera estratégica, por fases y con una planificación detallada. No es solo una sustitución de algoritmos, sino un rediseño progresivo de la infraestructura de seguridad para garantizar resiliencia ante la amenaza cuántica.



La estrategia debe considerar la evaluación de riesgos, selección de algoritmos, implementación escalonada y monitoreo continuo, siguiendo tres pilares: Identificar, Proteger y Gobernar.

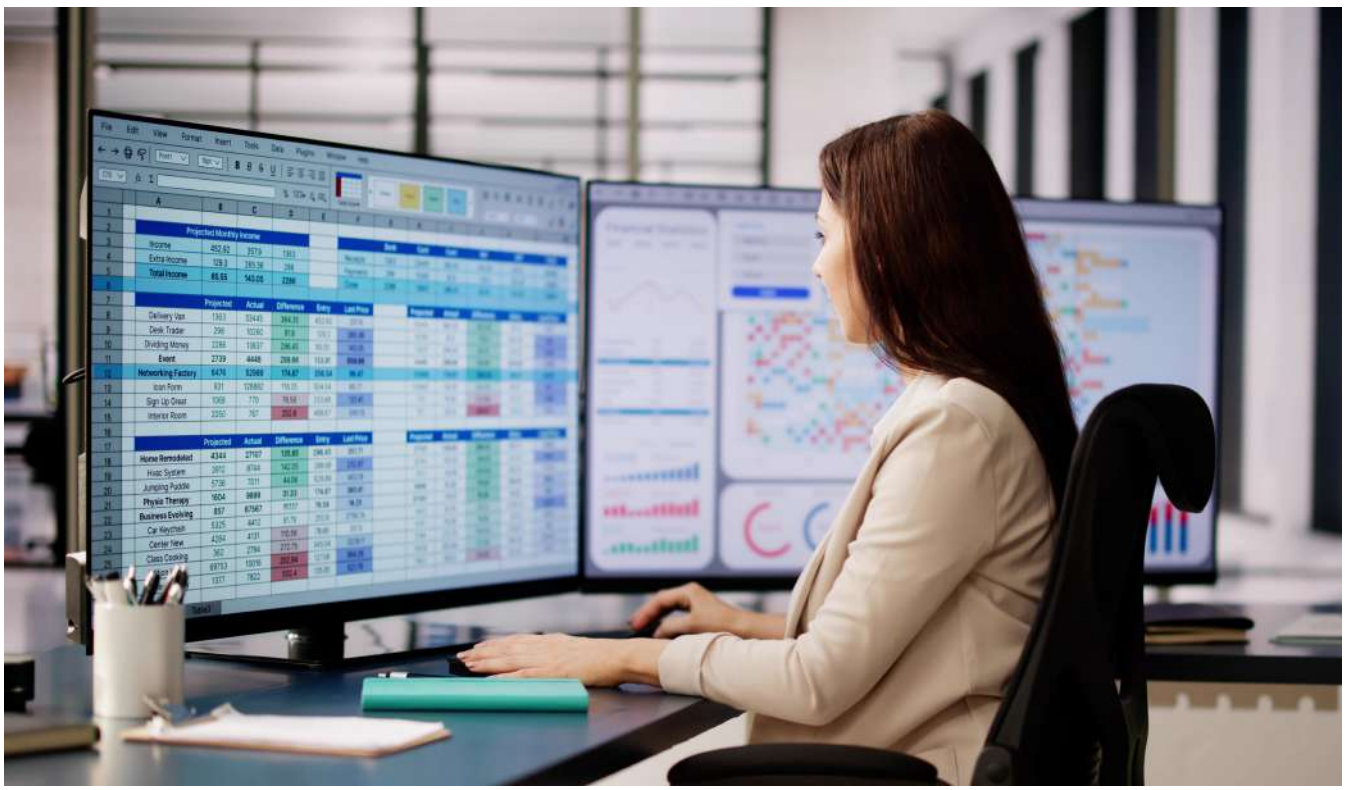
Pilar 1. Identificar: Inventario criptográfico y evaluación de riesgos

La evaluación de riesgos es un proceso continuo y dinámico que debe integrarse en la gestión de seguridad de la información de las empresas. Debe abarcar los siguientes aspectos clave:

Inventario de activos criptográficos

El primer paso es identificar y documentar todos los activos criptográficos de la organización para evaluar su exposición a la amenaza cuántica. Esto incluye:

- **Claves criptográficas**, que incluyen su tipo, longitud y algoritmo, utilizadas en sistemas, aplicaciones y dispositivos.
- **Certificados digitales que identifican** su emisor, fecha de expiración
  y los sistemas y aplicaciones dependientes.
- **Bibliotecas criptográficas,** sus versiones y las aplicaciones que las utilizan.
- Dependencias externas y servicios de terceros que utilizan criptografía vulnerable.
- **Protocolos criptográficos** utilizados, como TLS/SSL, SSH, IPsec, etc., incluyendo sus versiones.
- **Contexto de uso** para conocer qué y dónde se está utilizando.



La implementación de un **inventario criptográfico automatizado** es fundamental para comprender el nivel de exposición al riesgo y establecer prioridades en el proceso de migración hacia la criptografía poscuántica (PQC).

Se recomienda utilizar herramientas especializadas de **análisis de código estático y descubrimiento de claves** para garantizar una evaluación precisa y exhaustiva de los activos criptográficos. Este análisis debe incluir la **detección de prácticas de codificación inadecuadas**, como el uso de algoritmos criptográficos obsoletos, parámetros inseguros o claves con longitudes insuficientes.

Análisis de riesgos y gestión de vulnerabilidades

Una vez que se tiene un inventario criptográfico, el siguiente paso es evaluar los riesgos y gestionar las vulnerabilidades en función de:

- **Dependencias** para determinar qué sistemas, aplicaciones y procesos de negocio se relacionan con cada activo criptográfico.
- **Criticidad** según el tipo de información protegida e impacto de su exposición.
- **Vulnerabilidad** a ataques actuales como 'Harvest Now, Decrypt Later' y cuánticos, como los que utilizan RSA o ECC con longitudes de clave inadecuadas.
- **Prioridad** para migrar primero a PQC los activos más críticos según su riesgo, según la probabilidad de ocurrencia e impacto potencial.

Es fundamental integrar las fuentes IT relevantes, como sistemas de gestión de configuración (CMDB), registros de red y aplicaciones, para proporcionar el contexto necesario de los activos identificados. Esto facilita una correcta correlación entre los activos criptográficos y sus dependencias operativas, asegurando así una evaluación de riesgos más precisa y accionable.

En esta etapa es fundamental alinear la relevancia de la PQC con los objetivos estratégicos de la empresa. La planificación debe ser meticulosa, priorizando cuidadosamente qué abordar primero, ya que los cambios requieren tiempos significativos de implementación y adaptación.

Estrategia y hoja de ruta de la criptoagilidad

El análisis de riesgos culmina con un plan inicial de transformación que debe:

- **Definir principios arquitectónicos** para sistemas resistentes a cambios criptográficos, garantizando la capacidad de reemplazar algoritmos ágilmente.
- **Modernizar la infraestructura criptográfica** para asegurar compatibilidad y reducir riesgos operativos.
- **Actualizar servicios y aplicaciones** para integrarse con criptografía PQC.
- Implementar medidas de **protección para datos en uso y reposo,** utilizando tecnologías de computación confidencial y gestión del ciclo de vida de claves.
- **Definir una hoja de ruta detallada** con objetivos a corto y largo plazo, incluyendo métricas y metas específicas.

El enfoque debe ser progresivo, enfocándose primero en activos críticos y asegurando la continuidad operativa durante la transición.

En Telefónica Tech nos posicionamos como un socio integral, capaz de proporcionar una guía experta para ayudar a las organizaciones a definir y ejecutar este plan de transformación tecnológico. Con amplia experiencia en el campo de la criptoagilidad y un conocimiento profundo de los objetivos estratégicos del negocio, ofrecemos soluciones adaptadas a las necesidades específicas de cada empresa.

Con nuestro apoyo las organizaciones, empresas y administraciones públicas aseguran que la integración de la criptografía poscuántica (PQC) es efectiva, segura y está alineada con los objetivos de negocio, maximizando el retorno de la inversión y fortaleciendo la resiliencia operativa.

Pilar 2. Proteger: Implementación de soluciones y transición segura

La evaluación de riesgos es un proceso continuo y dinámico que debe integrarse en la gestión de seguridad de la información de las empresas. Debe abarcar los siguientes aspectos clave:

Adopción de iniciativas priorizadas

La implementación de PQC requiere realizar una adopción estratégica basada en las prioridades establecidas durante las fases anteriores. Este proceso debe incluir:

Pruebas piloto y de concepto (PoC)

Antes de una implementación a gran escala es fundamental realizar pruebas piloto en entornos controlados para validar las estrategias de transición, considerando:

- **Infraestructura**: Pruebas con distintos componentes de la infraestructura de comunicaciones (como gateways, túneles VPN, servidores TLS, etc.) para evaluar progresivamente la integración de algoritmos de criptografía poscuántica, garantizando la compatibilidad con sistemas heredados sin necesidad de cambios disruptivos

- **Aplicaciones**: Uso de servicios de Criptografía como Servicio (Crypto-as-a-Service, CaaS) para evaluar la integración de PQC.

- **Datos**: Ensayos con frameworks de gestión de claves empresariales (EKMF) para proteger datos en reposo y en tránsito.

Las pruebas piloto deben evaluar cuidadosamente las implicaciones de rendimiento, compatibilidad y posibles riesgos en un entorno controlado.

Implementación gradual y progresiva

La adopción progresiva de PQC garantiza una transición segura con mínimo impacto operacional.
Se recomienda:

- Revisar y ajustar los resultados de las pruebas piloto.
- Migrar primero comunicaciones críticas (VPN, TLS, SSH) usando protocolos híbridos.
- Modificar aplicaciones internas con impacto limitado en los servicios.
- Sustituir la criptografía en frontales expuestos a clientes.
- Retirar gradualmente algoritmos obsoletos en sistemas menos críticos.

Reevaluación e impacto

Durante y después de la implementación:

- Evaluar periódicamente el impacto en términos de rendimiento y compatibilidad.
- Actualizar políticas y métricas basadas en la experiencia obtenida.
- Ajustar el plan de transformación según la aparición de nuevas necesidades o amenazas.

Este proceso iterativo asegura la capacidad de adaptación a largo plazo.

Escenarios de aplicación

La transición a la criptografía poscuántica demanda atención específica en infraestructura, aplicaciones y datos, abordando amenazas cuánticas mientras se fomenta la soberanía digital.

Infraestructura

Comunicaciones seguras

- El uso de algoritmos híbridos en TLS y la adaptación de elementos de comunicaciones (VPN, gateways, etc.) con criptografía poscuántica son clave para proteger comunicaciones críticas frente a ataques cuánticos futuros.
- Los dispositivos IoT deben implementar soluciones ligeras compatibles con PQC para garantizar rendimiento y seguridad.

Infraestructura robusta frente a ataques cuánticos

- Incorporar módulos de seguridad de hardware (HSM) actualizables para soportar algoritmos PQC.
- Actualizar infraestructuras de clave pública (PKI) para manejar certificados híbridos.

Nube soberana

- Garantizar el control local de claves criptográficas y datos almacenados dentro de las fronteras nacionales, cumpliendo con regulaciones específicas.

Aplicaciones

El ámbito de las aplicaciones debe considerar aspectos como:

- **Firma digital poscuántica**: Implementar algoritmos como CRYSTALS-Dilithium o FALCON para asegurar la integridad de procesos críticos y respaldar firmas electrónicas avanzadas.
- **Integración nativa de criptografía**: Actualizar las aplicaciones empresariales para interoperar con soluciones externas y modulares de criptografía ágil

Datos

La soberanía de los datos es esencial para garantizar la seguridad y cumplimiento normativo:

Protección de datos soberanos

- Asegurar que los datos se almacenen y procesen bajo jurisdicciones específicas.
- Aplicar criptografía poscuántica tanto en tránsito como en reposo, integrando el manejo local de claves resistentes a ataques cuánticos. Esto no solo mitiga amenazas como *Harvest Now, Decrypt Later*, sino que también garantiza la soberanía sobre los datos, al mantener el control exclusivo de las claves sin depender de terceros o entornos externos.

Estos escenarios garantizan un enfoque holístico que protege activos, optimiza recursos y fomenta la autonomía digital durante la transición a PQC.

Impacto en el rendimiento y consideraciones específicas para IoT

La transición a PQC impactará el rendimiento de los sistemas debido a la mayor complejidad computacional de los algoritmos poscuánticos. Es necesario evaluar y mitigar este impacto mediante:

- **Selección de algoritmos** optimizados que equilibren seguridad y eficiencia para mantener el rendimiento de los sistemas durante la transición.
- **Implementaciones** optimizadas en software y hardware para una transición más fluida y eficiente.
- **Uso de aceleradores criptográficos** específicos para optimizar la ejecución de algoritmos criptográficos y mejorar tiempos de ejecución.
- **Arquitecturas híbridas** que combinen criptografía clásica y poscuántica mientras se completa la transición para incorporar gradualmente los nuevos algoritmos de PQC, manteniendo los sistemas existentes.

Pilar 3. Gobernar: Implementación y seguimiento continuo

La gobernanza establece las bases para gestionar la transición a la criptografía poscuántica de manera estructurada y eficiente.

Esta etapa busca implementar las capacidades necesarias para garantizar la seguridad criptográfica a largo plazo, adaptándose a los cambios tecnológicos y alineándose con los objetivos empresariales.

La gobernanza incluye la coordinación interna y la interoperabilidad con sistemas existentes. Esto permite ajustar y mejorar la infraestructura criptográfica de manera continua.

Centro de Excelencia en Criptografía

Se recomienda establecer un Centro de Excelencia de Criptografía (CCoE) o un equipo dedicado responsable de:

- Mantenerse al día con la evolución de la computación cuántica y la PQC, ya que la investigación en ambos campos es continua.
- Evaluar el impacto potencial de la computación cuántica en la empresa considerando diversos escenarios y plazos.
- Definir y mantener actualizada la política criptográfica de la empresa, incluyendo la transición a PQC.
- **Identificar los activos críticos que requieren migración prioritaria,** incluyendo sistemas y datos vulnerables que necesitan migración urgente a PQC.

El Centro de Excelencia de Criptografía (CCoE) de Telefónica ha implementado estrategias criptográficas avanzadas para proteger sus activos digitales. Se enfoca en tres áreas: comunicaciones y ciberseguridad, computación y simulación, y sensórica y metrología para aprovechar la computación cuántica y mejorar la seguridad de las redes y sistemas de la compañía y sus clientes.

Este equipo gestiona y asegura las claves criptográficas de la empresa, lidera la adopción de tecnologías PQC y desarrolla normativas internas para aplicar una estrategia de criptoagilidad para proteger los sistemas e infraestructuras.

Además, el CCoE de Telefónica colabora con entidades reguladoras y participa en iniciativas globales, y asegura que la empresa esté lista para enfrentar amenazas cuánticas futuras y cumplir con los estándares de seguridad más estrictos.

Visibilidad de extremo a extremo

La visibilidad de extremo a extremo (E2E) en criptografía es fundamental para minimizar riesgos, controlar la superficie de ataque y facilitar decisiones estratégicas, tácticas y normativas. Ofrece una visión comprensiva de todos los activos criptográficos, como claves, certificados, bibliotecas y protocolos.

Componentes clave de la visibilidad E2E

- **Herramientas de descubrimiento automatizado**: Identifican activos criptográficos y detectan configuraciones erróneas, uso de algoritmos obsoletos o claves vulnerables.
- **Gestión centralizada y modular de activos criptográficos**: Permite una detección temprana de vulnerabilidades y facilita la respuesta rápida a amenazas.
- **Integración con sistemas de seguridad (SIEM, SOAR)**: Vincula la visibilidad criptográfica con plataformas de gestión para correlacionar eventos y analizar riesgos.
- **Monitorización continua**: Garantiza que los activos criptográficos estén actualizados y seguros mientras detecta nuevos riesgos.

Beneficios clave

- **Control proactivo de riesgos**: Identifica y atiende prioridades críticas.
- **Optimización de recursos**: Centraliza la gestión para reducir duplicidades y mejorar la asignación de recursos.
- **Soporte estratégico**: Proporciona información precisa para planificar inversiones y tomar decisiones informadas.

La visibilidad de extremo a extremo es la base para implementar medidas de seguridad robustas y garantizar la transparencia en la gestión criptográfica.

Criptoagilidad

La criptoagilidad garantiza la capacidad de adaptarse rápidamente a nuevas amenazas y cambios en los estándares criptográficos sin comprometer la operatividad.

Este enfoque también incluye los servicios gestionados y la respuesta ante incidentes para una gestión integral de la seguridad.

Servicios gestionados

- **Centralización criptográfica**: Implementar Criptografía como Servicio (CaaS) permite facilitar operaciones criptográficas empleando interfaces API estándar.
- **Automatización de procesos**: Incluye la gestión de claves, certificados y algoritmos para evitar errores manuales.
- **Escenarios complejos gestionados**: Manejo eficaz de identidades y criptografía en entornos híbridos o distribuidos.

Respuesta ante incidentes

La capacidad de gestionar incidentes criptográficos de forma ágil es crítica para mitigar riesgos. Esto implica:

- **Planes específicos de respuesta**: Procedimientos claros para identificar, contener y mitigar incidentes relacionados con PQC.
- **Incorporación de criptoagilidad**: Permite la rápida actualización de algoritmos en caso de vulnerabilidades.
- **Simulacros y entrenamiento**: Realizar prácticas periódicas para evaluar la preparación y eficacia del plan de respuesta.

Beneficios clave de la criptoagilidad

- **Compatibilidad sin interrupciones**: Protección de aplicaciones y redes sin necesidad de modificar código ni revisar arquitecturas fundamentales.
- **Interoperabilidad a largo plazo**: Soporte de PKI híbridas y arquitectura modular para facilitar cambios futuros sin interrupciones operativas.
- **Resiliencia operativa**: La integración de criptoagilidad en los sistemas garantiza una actualización constante frente a nuevas amenazas.

La criptoagilidad permite a las organizaciones mantenerse protegidas frente a vulnerabilidades y nuevas amenazas sin afectar su capacidad operativa.

Casos de uso sectoriales

La amenaza de la computación cuántica y la necesidad de la criptografía poscuántica no son abstractas: tienen implicaciones concretas y significativas para diversas industrias. Algunos ejemplos:

Sector financiero

- **Amenaza:** Las instituciones financieras (bancos, bolsas de valores, compañías de seguros) dependen en gran medida de la criptografía para proteger las transacciones, la información de los clientes y los activos financieros.
- **Aplicaciones PQC:**
    - **Comunicaciones seguras:** Protección de las comunicaciones entre bancos, clientes y otras instituciones financieras utilizando TLS/SSL con algoritmos PQC.
    - **Firmas digitales:** Asegurar la integridad y autenticidad de las transacciones financieras utilizando firmas digitales PQC.
    - **Blockchain y criptomonedas:** Las redes blockchain y criptomonedas que utilizan algoritmos criptográficos vulnerables como ECDSA o RSA deberán migrar a algoritmos PQC como Dilithium para mantener su seguridad.
    - **Protección de datos en reposo:** Cifrado de bases de datos y archivos que contienen información financiera sensible utilizando algoritmos PQC.
- **Cumplimiento:** Las regulaciones financieras (como PCI DSS, PSD2 en Europa, y otras normativas) exigirán, cada vez más, el uso de criptografía resistente a la computación cuántica.

Sector Salud

- **Amenaza:** Los hospitales, clínicas, compañías de seguros de salud y laboratorios manejan grandes cantidades de información médica confidencial (historiales clínicos, datos genómicos, resultados de pruebas).

  La exposición de esta información podría tener graves consecuencias para la privacidad de los pacientes y la reputación de las instituciones.

- **Aplicaciones PQC:**
    - **Protección de historias clínicas electrónicas (EHR):** Cifrado de EHR utilizando algoritmos PQC para proteger la confidencialidad de la información del paciente.
    - **Comunicaciones seguras:** Protección de las comunicaciones entre médicos, pacientes y otros profesionales de la salud (telemedicina, correo electrónico seguro) utilizando TLS/SSL con algoritmos PQC.
    - **Intercambio seguro de información:** Facilitar el intercambio seguro de información médica entre diferentes instituciones utilizando protocolos y formatos de datos compatibles con PQC.
    - **Investigación genómica:** Protección de datos genómicos, que son altamente sensibles, como es el caso de nodos genómicos nacionales, y tienen un valor a largo plazo, utilizando algoritmos PQC.
- **Cumplimiento:** Regulaciones como HIPAA en EE UU y GDPR en Europa exigen la protección de la información médica. La PQC será esencial para cumplir con estas regulaciones en la era cuántica.

Sector gubernamental y defensa

- **Amenaza:** Los gobiernos y las agencias de defensa manejan información clasificada de alto valor, incluyendo secretos de estado, comunicaciones militares o datos de inteligencia.

  La exposición de esta información podría tener consecuencias devastadoras para la seguridad nacional.

- **Aplicaciones PQC:**
    - **Comunicaciones clasificadas:** Protección de las comunicaciones clasificadas (voz, datos, video) utilizando algoritmos PQC.
    - **Gestión centralizada de las claves criptográficas:** Las claves criptográficas clásicas y poscuánticas son esenciales para la seguridad y la criptoagilidad
    - **Cifrado de datos en reposo:** Cifrado de bases de datos y archivos que contienen información clasificada utilizando algoritmos PQC.
    - **Sistemas de defensa:** Asegurar la integridad y autenticidad de los sistemas de defensa y otros sistemas críticos utilizando firmas digitales PQC.
    - **Infraestructura crítica:** Protección de la infraestructura crítica (redes eléctricas, sistemas de transporte, etc.) contra ataques cuánticos utilizando PQC.
- **Cumplimiento:** Los gobiernos y las agencias de defensa adoptarán PQC debido a la necesidad de proteger la seguridad nacional.

Sector de la automoción

- **Amenaza:** Los sistemas de los vehículos modernos son altamente dependientes de software, con comunicaciones internas y externas.

  Un ciberataque podría comprometer la seguridad de los ocupantes.

- **Aplicaciones PQC:**
  - **Comunicaciones V2V y V2I:** Protección de las comunicaciones Vehículo a Vehículo y Vehículo a Infraestructura para asegurar la integridad de los datos y evitar ataques maliciosos.

  - **Actualizaciones de software:** Se debe asegurar la integridad de las actualizaciones para evitar modificaciones maliciosas.

Industria 4.0

- **Amenaza:** La industria 4.0 hace un gran uso de IoT en todos sus procesos. Estos dispositivos suelen ser de bajos recursos y con poca capacidad de cómputo que operan en entornos complejos.

- **Aplicaciones PQC:**
  - **Comunicaciones M2M:** Protección de las comunicaciones máquina a máquina.

  - **Control de la cadena de suministro:** Asegurar la integridad de los procesos.

Conclusiones y recomendaciones para asegurar el futuro digital en la era cuántica

Este documento ha explorado la inminente amenaza de la computación cuántica para la criptografía actual, la necesidad crítica de la criptografía poscuántica y las estrategias necesarias para una transición segura y eficaz.

Necesidad de la acción

La transición hacia la criptografía poscuántica es una necesidad inmediata, debido a tres razones fundamentales:

- **La criptografía como pilar de la soberanía digital**: En un entorno digital cada vez más interconectado y cambiante, la criptografía no solo garantiza la confidencialidad e integridad de la información, sino que es un elemento clave para **preservar la autonomía tecnológica y la soberanía sobre los datos.** Frente a la amenaza que representan los futuros ordenadores cuánticos, la adopción de criptografía poscuántica (PQC) se vuelve estratégica para evitar la dependencia de tecnologías vulnerables o controladas por terceros, y así asegurar el control pleno y resiliente sobre los activos digitales críticos.

- **La amenaza real de la computación cuántica**: los algoritmos actuales como RSA y ECC podrían quedar comprometidos en menos de una década debido a los avances en computación cuántica, destacando la importancia de actuar ahora para proteger la información sensible y confidencial.

- **La criptografía poscuántica como solución**: ofrece algoritmos capaces de resistir tanto a los ordenadores clásicos como cuánticos, implementables hoy en día con tecnología convencional, reduciendo así la ventana de vulnerabilidad ante ataques futuros.

Dado este contexto, la urgencia en la adopción de criptografía poscuántica es innegable.

Recomendaciones finales y acciones efectivas

Las siguientes recomendaciones profundizan en estrategias esenciales para asegurar un futuro digital robusto en la era cuántica. Las organizaciones deben enfocarse en:

- **Evaluación y gestión continuas del riesgo criptográfico**, estableciendo un inventario criptográfico exhaustivo, automatizado y actualizado.

- **Implementación gradual y criptoagilidad**, adaptando arquitecturas tecnológicas modulares para permitir cambios rápidos de algoritmos criptográficos, facilitando así la adaptación continua ante futuras amenazas.

- **Fortalecimiento de la gobernanza criptográfica**, a través de la creación de un Centro de Excelencia en Criptografía (CCoE), garantizando el liderazgo y supervisión de la transición hacia PQC, así como el cumplimiento normativo actual y futuro.

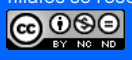
Adicionalmente, se recomienda desarrollar un plan detallado de transformación basado en la evaluación de riesgos, realizar pruebas piloto previas a la implementación a gran escala y asegurar la formación continua del personal implicado en esta transición estratégica.

> Para garantizar una transición efectiva a la criptografía poscuántica, se recomienda comenzar hoy mismo: con una evaluación de riesgos, un inventario criptográfico, y pruebas piloto con algoritmos PQC estandarizados por el NIST.
> La criptoagilidad es esencial.

Sobre Telefónica Tech

Telefónica Tech es la compañía líder en transformación digital. La compañía cuenta con una amplia oferta de servicios y soluciones tecnológicas integradas de Ciberseguridad, Cloud, IoT, Big Data, Inteligencia Artificial y Blockchain.

telefonicatech.com



Telefónica Tech