

Ciberseguridad y Resiliencia

RIESGO CRIPTOGRÁFICO EN UN MUNDO POST-CUÁNTICO

INFORMACIÓN	Empresa: MAPFRE Página web: www.mapfre.com Categoría IV Certamen Forbes a la Innovación by Kyndryl: Proyecto de Nuevas Tecnologías – Ciberseguridad
BREVE DESCRIPCIÓN DEL PROYECTO	Proyecto para evaluar el impacto de la computación cuántica en la criptografía de MAPFRE, identificando riesgos y priorizando acciones usando un Mapa de Calor Quantum Safe5. Define áreas críticas, iniciativas clave y el roadmap para la transición segura hacia criptografía post cuántica.
PROBLEMA IDENTIFICADO	Aunque existan varios campos donde la computación cuántica conllevará mejoras sustantivas, el campo de la criptografía ha despertado especial interés ya que los avances en la computación cuántica van a suponer un cambio significativo en la criptografía. Este hecho no es nuevo, sino que teóricamente se publicó a mediados de los 90, si bien en aquellos tiempos no existía ningún ordenador cuántico. La criptografía es la base de la seguridad y la confianza en Internet en los últimos 30 años por lo que la transición de las empresas a nuevas formas de cifrado no va a ser un camino fácil. Se estima que al menos serán necesarios 10 años para acometer los proyectos de inventariado, cambios HW y SW y la refactorización de aplicaciones, lo cual unido a lo incierto de la eficacia y la falta de confianza en los nuevos algoritmos PQC está provocando inacción por parte de las organizaciones. Una amenaza como la computación cuántica con capacidad real de retar los esquemas criptográficos actuales, tendrá un efecto destabilizador significativo en el sector financiero y por ende en la economía mundial, ya que los estados financieros y las transacciones con tarjeta podrían ser falseados por un tercero con acceso a esta tecnología.

Ciberseguridad y Resiliencia

RIESGO CRIPTOGRÁFICO EN UN MUNDO POST-CUÁNTICO

SOLUCIÓN PROPUESTA

Es necesario entender el uso actual de la criptografía dentro de MAPFRE y el posible impacto que sobre ella tendrá la computación cuántica para determinar y visualizar la estrategia segura de transformación hacia una entidad Quantum Safe.

Mediante este proyecto, identificamos áreas clave de acción. Utilizando diferentes mecanismos y la captura de información, MAPFRE ha definido un mapa de calor Quantum Safe que identifica aquellos entornos tecnológicos que tienen un mayor riesgo ante una vulneración de la criptografía actual y, por tanto, una mayor prioridad en la adopción de mecanismos y algoritmos de criptografía post-cuántica.

VALORES DIFERENCIALES

Innovación

Mapa de Calor Quantum Safe para cuantificar el riesgo criptográfico por dominios y procesos críticos, priorizando dónde actuar primero.

Impacto

Criterios de priorización de actuaciones ligadas al impacto económico en los procesos de negocio.

Gobierno

La criptografía es el pilar fundacional de la seguridad en cualquier compañía y conocer dónde y cómo se usa es vital en un mundo post-cuántico.

Criptoagilidad en Plataformas

La centralización de los servicios criptográficos en las nuevas plataformas corporativas donde se desarrollan las apps del futuro facilita la agilidad en el cambio de cualquier algoritmo cuando la computación cuántica sea una realidad.

Ciberseguridad y Resiliencia

RIESGO CRIPTOGRÁFICO EN UN MUNDO POST-CUÁNTICO

	Ecosistema Cambiar la criptografía no es posible sin la colaboración y participación del ecosistema de fabricantes, proveedores y socios e incluso clientes que forman parte de la cadena de valor de la compañía.
--	--

INDICADORES DE ÉXITO	Indica los datos cuantificables para cada uno de los puntos: • Número de personas afectadas por la iniciativa: 30 Millones de clientes en todo el mundo, 30K empleados, 4500 oficinas en 38 países • Número de instituciones afectadas por la iniciativa: 135.000 proveedores y 87.000 empresas distribuidoras • Impacto económico en países, ciudades, ayuntamientos, agrupaciones profesionales o empresas: +33.000 Millones de euros en primas de productos aseguradores a clientes protegidos con criptografía. Existen pocos aspectos de la ciberseguridad con mayor impacto en una organización que la criptografía. Es la base fundacional de la protección de toda la información de nuestros clientes y socios y de los procesos de negocio de MAPFRE.
PLATAFORMAS Y TECNOLOGÍAS UTILIZADAS	• Infraestructura de clave pública (PKI) de Microsoft • Certificados X.509 FNMT-RCM • Plataformas de gestión de certificados X.509: AWS Certificate Manager, NebulaCert • Hardware Security Module nCipher/nShield • Algoritmos criptográficos PQC NIST FIPS 203, 204, 205 y 206 • Plataformas de gestión de claves criptográficas: AWS KMS, Azure KeyVault, OCI Vault, IGKLM

Ciberseguridad y Resiliencia

RIESGO CRIPTOGRÁFICO EN UN MUNDO POST-CUÁNTICO

IMPACTO EN SOSTENIBILIDAD	En el aspecto ambiental, mediante este proyecto se pretende racionalizar el uso de la criptografía a nivel corporativo (cierre de algoritmos inseguros y ajuste de parámetros criptográficos) reduciendo ciclos de cómputo por transacción a la par que se mejora la confidencialidad de la información y decomisionando hardware criptográfico legacy con menor eficiencia energética. Se ha incluido como criterio de diseño del plan de migración a PQC: no empeorar la huella compensando con optimización y aceleración HW. En el aspecto social, la protección de los datos más longevos de las personas (salud, finanzas) frente al riesgo harvest-now, decrypt-later, hace efectivo el propósito de MAPFRE de cuidar de las personas protegiendo también su información. Por último, este proyecto nos permite mejorar el gobierno del uso de la criptografía aplicando un nivel de control mayor sobre el nivel de protección de la información y garantizando el cumplimiento de los requisitos de los reguladores en esta materia (DORA/ENS/NIS2)
IMPACTO EN LA ESTRATEGIA DE LA COMPAÑÍA	La misión de MAPFRE es ser la aseguradora de confianza para nuestros clientes. Mediante este proyecto reforzamos la propuesta de valor en todos los canales digitales facilitando el time-to-market de productos que requieren confianza digital sin la cual no es posible realizar ninguna transacción. De manera adicional, mediante este proyecto mejoramos el cumplimiento de la normativa, la resiliencia operativa y la continuidad de negocio disminuyendo el riesgo sistémico por ruptura criptográfica en los procesos de negocio core.

Ciberseguridad y Resiliencia

RIESGO CRIPTOGRÁFICO EN UN MUNDO POST-CUÁNTICO

MÁS INFORMACIÓN DE INTERÉS DEL PROYECTO

Mediante este proyecto una gran corporación multinacional como MAPFRE ha conseguido transformar la preocupación por el riesgo de la computación cuántica en un plan de acción medible. MAPFRE ha conseguido controlar dónde y cómo se usa la criptografía en la corporación, definiendo una hoja de ruta PQC priorizada por impacto de negocio evitando dependencias de fabricantes (lock-in).

La criptografía está embebida en todo sistema tecnológico y es el pilar fundacional de la seguridad. Cuando haya que cambiar los algoritmos (y habrá que cambiarlos) en MAPFRE este cambio afecta a todo el ecosistema tecnológico que abarca más de 11.000 servidores repartidos en siete grandes centros de procesos de datos y tres proveedores cloud; más de 50.000 puestos repartidos en 28 países; 85.000 workloads en más de 10 regiones diferentes de tres proveedores cloud y más de 1.000 aplicaciones