Telefónica

Evaluación de proveedores: preparación para la era cuántica

Introducción

La transición hacia la criptografía poscuántica introduce un nuevo riesgo en la gestión de proveedores tecnológicos. En entornos Cloud y servicios digitales, gran parte de la postura de seguridad depende de terceros sobre los que no se tiene control directo.

Este cuestionario proporciona un marco estructurado para evaluar el nivel de preparación de proveedores frente a amenazas cuánticas. Incorpora criterios técnicos, operativos y de gobernanza. Su objetivo es facilitar la toma de decisiones en procesos de selección, contratación y revisión periódica.

Las preguntas se organizan por dominios clave e incluyen niveles de prioridad para orientar su aplicación práctica. Todas las respuestas deben incluir evidencias técnicas para validar la información y asegurar su trazabilidad.

Más en Evaluación de proveedores Cloud 'quantum-readiness': marco de auditoría y cuestionario técnico.

Resumen

El siguiente cuestionario está estructurado en cuatro dominios. Cada pregunta incluye una clasificación de prioridad:

- **CRÍTICA** (debe responderse antes de contratar o renovar).
- **ALTA** (debe responderse en los primeros 90 días).
- **MEDIA** (importante para la madurez del programa).

NOTA: Esta guía tiene carácter orientativo y podrá adaptarse en función de las necesidades específicas y de los objetivos de análisis, considerando aspectos relacionados con la infraestructura, la arquitectura de red, la seguridad y las aplicaciones.

Todas las respuestas deberán complementarse con las evidencias técnicas correspondientes, de manera que se garantice la adecuada trazabilidad de los servicios incluidos en el alcance.

Dominio 1: criptografía y algoritmos Qué protege los datos y con qué		
1	¿Qué algoritmos criptográficos utiliza actualmente para cifrado en tránsito (TLS) y en reposo? ¿Tienen documentado el inventario criptográfico de su plataforma?	**CRÍTICA**
2	¿Existe una hoja de ruta formal para la migración a algoritmos poscuánticos (NIST PQC: ML-KEM, ML-DSA, SLH-DSA)?	**CRÍTICA**
3	¿Soportan o tienen planificado soporte para TLS 1.3 con extensiones KEM poscuánticas (hybrid key exchange)?	**ALTA**
4	¿Han realizado un crypto-agility assessment de su plataforma? ¿Con qué periodicidad actualizan los algoritmos criptográficos?	**ALTA**
5	¿Qué longitudes de clave utilizan actualmente? ¿Soportan RSA-4096 o ECC P-384 como medida transitoria?	**MEDIA**

Dominio 2: gestion de claves y datos Quién controla las claves y cómo		
1	¿Ofrecen la opción de gestión de claves por el cliente (BYOK / HYOK)? ¿Sobre qué infraestructura HSM?	**CRÍTICA**
2	¿Los módulos HSM utilizados están certificados FIPS 140-3? ¿Tienen planes de certificación para HSM con soporte PQC nativo?	**CRÍTICA**
3	¿Cómo garantizan que los datos almacenados no pueden ser capturados por terceros para descifrado posterior (HNDL)? ¿Existe aislamiento criptográfico entre tenants?	**CRÍTICA**
4	¿Cuál es la política de retención de datos cifrados tras la finalización del contrato? ¿Se garantiza la destrucción criptográfica?	**ALTA**
5	¿Ofrecen registros auditables de todas las operaciones de acceso y uso de claves criptográficas?	**MEDIA**

Dominio 3: operaciones y resiliencia criptográfica Qué pasa cuando algo cambia		
1	¿Tienen un plan documentado de respuesta ante la posibilidad de que un algoritmo criptográfico actualmente en uso resulte comprometido?	**CRÍTICA**
2	¿Cuál es el SLA para actualizar o reemplazar un algoritmo criptográfico si NIST o ENISA emiten una alerta de vulnerabilidad?	**ALTA**
3	¿Participan en programas de estandarización o grupos de trabajo de criptografía poscuántica (ETSI QKD ISG, IETF, Cloud Security Alliance PQC)?	**ALTA**
4	¿Se realizan pruebas de penetración específicas sobre infraestructura criptográfica? ¿Con qué frecuencia y por quién?	**MEDIA**
5	¿Notifican proactivamente a los clientes cuando se realizan cambios en los algoritmos o protocolos criptográficos de la plataforma?	**MEDIA**

Dominio 4: gobernanza y cumplimiento Compromiso institucional con la transición		
1	¿Han publicado o tienen disponible bajo NDA una política formal de quantum-readiness o PQC migration roadmap?	**CRÍTICA**
2	¿Están alineados con los marcos regulatorios europeos relevantes (NIS2, DORA, ENS) en su estrategia criptográfica?	**ALTA**
3	¿Existen cláusulas contractuales que garanticen la actualización criptográfica dentro de plazos definidos? ¿Están dispuestos a incorporarlas?	**ALTA**
4	¿Tienen identificado un responsable o equipo dedicado a la gestión de la transición poscuántica dentro de su organización?	**MEDIA**
5	¿Comparten con clientes los resultados de auditorías de seguridad criptográfica realizadas por terceros independientes?	**MEDIA**

Sistema de puntuación para tomar decisions

Ante la necesidad de comparar proveedores o decidir si renovar un contrato existente, un sistema de puntuación simple puede estructurar la decisión. Asigna 2 puntos por cada pregunta CRÍTICA respondida satisfactoriamente, 1 punto por cada ALTA y 0,5 por cada MEDIA.

El máximo posible con este cuestionario es 16 puntos.

PUNTOS	CATEGORÍA	ACCIÓN
>13	**Proveedor quantum-aware** Tiene programa activo, documentación y disposición contractual. Proceder con negociación de cláusulas específicas.	CONTRATAR
8 - 12	**Proveedor en transición** Conciencia del problema, pero sin programa maduro. Exigir hoja de ruta con hitos verificables como condición contractual.	CONDICIONAL
0 - 7	**Proveedor no preparado** Ausencia de conciencia o programa. Riesgo material para activos de datos con valor a largo plazo. Reconsiderar o exigir compromisos vinculantes.	REVISAR

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