TXDXSECURE

2025

CRYPTOGRAPHY AGILE

NUESTRA SOLUCIÓN

Este servicio está diseñado para ayudar a las organizaciones a migrar de manera segura y eficiente de las suites criptográficas clásicas a las soluciones de criptografía post-cuántica (PQC). Ante la creciente amenaza de ataques "Cosecha ahora, descifrado después", es crucial adoptar medidas proactivas que garanticen la seguridad de los datos en el futuro.

BASES DEL SERVICIO

Criptografía Postcuántica (PQC)

Implementación de tecnologías que aseguran la resistencia de algoritmos criptográficos a ataques de computación cuántica.

Cumplimiento con NIST CSF 2.0

Alineación con el marco de ciberseguridad de NIST, siguiendo prácticas de identificación, protección, detección, respuesta y recuperación.

Recomendaciones de Palo Alto y Cisco

Optimización de soluciones de seguridad con mejores prácticas en firewalls, routers y switches.

ACCIONES DE IMPLEMENTACIÓN

1. EVALUACIÓN DE RIESGOS Y NECESIDADES

- Realizamos un análisis exhaustivo de los activos digitales y sus requisitos de seguridad.
- Identificamos los tipos de datos que requieren protección a largo plazo (datos financieros, PII).

2. DESARROLLO DE PLAN INTEGRAL (HLD)

- Establecemos una hoja de ruta para la migración a PQC, que incluya tiempos estimados y recursos necesarios.
- Se forma un equipo de gestión de proyectos para coordinar las actividades de migración.
- Estrategia para la migración a algoritmos postcuánticos y roadmap de transición.

3. INVENTARIO CRIPTOGRÁFICO

- Elaboramos un inventario completo de todos los dispositivos, aplicaciones y sistemas en la red, incluyendo detalles sobre los métodos de cifrado utilizados.
- Priorizamos componentes en función de la vulnerabilidad y criticidad para el negocio.

4. PRUEBA DE CONCEPTO (POC)

- Simulación del comportamiento de nuevos algoritmos y validación mediante pruebas de penetración.

5. NETWORK IMPLEMENTATION PLAN (NIP)

- Definición de la estrategia de implementación manteniendo los servicios activos.

6. IMPLEMENTACIÓN DE SOLUCIONES POSTCUÁNTICAS

- **Despliegue de Algoritmos PQC en Redes:** Implementación de algoritmos de criptografía post-cuántica (PQC) en dispositivos de red para garantizar la protección contra amenazas futuras.
- **Cumplimiento con Estándares de Seguridad (RFC 6379):** Configuración de las Suites Criptográficas Suite B para IPSec, reemplazando AES-128 por Suite-B-GCM-256 para aumentar la seguridad.
- **Actualización de Certificados y Claves (CA):** Migración a claves RSA de 4K y actualización de certificados VPN para cumplir con los estándares más recientes.
- **Mejora de Algoritmos de Hash:** Reemplazo de algoritmos de hash vulnerables, como MD5 y SHA-1, por SHA-384 o SHA-512, asegurando una mayor integridad en los datos.
- **Implementación de VPN Postcuánticas:** Integración de estándares (RFC 8784, 9242, 9370) para fortalecer las VPN.
- **Revisión de Conexiones SSL/TLS:** Actualización a TLSv1.3 con Perfect Forward Secrecy (PFS) para proteger las sesiones VPN y adopción de aplicaciones de escritorio con soporte para proxy inverso.
- **Enfoque de Claves Híbridas:** Combinación de algoritmos robustos como Group Diffie-Hellman con PQC para una mayor resistencia ante posibles ataques cuánticos.
- **Configuración de Redes y VPN Seguras:** Uso de IKEv2 y protocolos relevantes (como RFC 8784) para garantizar la seguridad de las redes y VPN.

7. PRUEBAS Y VALIDACIÓN

- Realizamos pruebas de resistencia y validación de las nuevas soluciones de cifrado en entornos controlados antes de la implementación en producción.
- Nos aseguramos de que las soluciones sean compatibles con los estándares establecidos por NIST y otras regulaciones pertinentes.

8. MONITOREO Y MANTENIMIENTO

- Establecemos una hoja de ruta para la migración a PQC, que incluya tiempos estimados y recursos necesarios.
- Se forma un equipo de gestión de proyectos para coordinar las actividades de migración.
- Estrategia para la migración a algoritmos postcuánticos y roadmap de transición.

ENTREGABLES

- Detalles de análisis y soluciones implementadas, incluyendo comparativas de estado.
- Presentación Kick Off "Análisis de Gobernanza" (PAG)
- Documento de Relevamiento de Información (SRD)
- Documento de Diseño de Alto Nivel (HLD)
- Documento de Pruebas Operacionales Simplificadas (LABTEST)
- Documento de Plan de Implementación (NIP)
- Documento de Informe final (DIF)

TXDXSECURE S.A.C.
RUC: 20607043427
Contáctanos: +51 942 325 448; +51 999 379 845
Correo: administracion@txdxsecure.com

Calle las Gorsellas No 167 Naranjal
San Martín de Porres
Lima, Perú

www.txdxsecure.com

2025