GUIA PRACTICA · DESCARGA GRATUITA

Plan de Migracion Post-Cuantica

para tu Empresa: 2025 · 2026 · 2027

Inventario criptografico · Matriz de riesgo · Cronograma de accion

Los ordenadores cuanticos aun no existen. Pero el ataque ya ha empezado. El modelo Harvest Now Decrypt Later implica que actores con recursos suficientes estan recopilando hoy trafico cifrado para descifrarlo en el futuro. Esta guia te da las tres herramientas esenciales para empezar a actuar ahora.

01 · INVENTARIO CRIPTOGRAFICO

Cataloga todos los sistemas que usan criptografia. Anota el algoritmo actual y su nivel de riesgo cuantico.

Sistema / Protocolo	Algoritmo actual	Riesgo cuantico	Prioridad
Servidor web HTTPS	TLS 1.3 + ECDSA P-256	Media (ECC)	**Alta**
VPN corporativa	IKEv2 + RSA-2048	ALTA (RSA)	**Urgente**
Firma de codigo	RSA-2048 o ECDSA	ALTA	Urgente
Cifrado de archivos	AES-256-GCM	Baja	Normal
Correo S/MIME	RSA-2048	ALTA	Alta
PKI interna	RSA-2048 / ECDSA	ALTA	Alta
SSH	ED25519 / RSA	Media / Alta	Alta
Tokens JWT	HMAC-SHA256	Baja	Normal

CHECKLIST INMEDIATO

- [ ] Listar todos los servicios con TLS/SSL activo
- [ ] Verificar version de TLS: minimo 1.2, recomendado 1.3
- [ ] Identificar certificados RSA y su fecha de caducidad
- [ ] Eliminar algoritmos obsoletos: MD5, SHA-1, DES, RSA < 2048 bits
- [ ] Cifrar archivos sensibles con AES-256-GCM (ver herramienta abajo)
- [ ] Inventariar proveedores con acceso a datos sensibles

Herramienta recomendada: ChacalCrypt (AES-256-GCM + Argon2) chacalsecurity.com/chacalcrypt.html

02 · MATRIZ DE RIESGO CRIPTOGRAFICO

Clasifica tus datos segun vida util y nivel de exposicion. Cuadrante superior derecho = prioridad maxima de proteccion.

	VIDA UTIL CORTA (< 5 anos)	VIDA UTIL LARGA (> 5 anos)
EXPOSICION ALTA	RIESGO MEDIO - Correos con estrategia operativa - Comunicaciones con clientes - Credenciales temporales Accion: migrar a hibrido en Fase 2	RIESGO CRITICO - Propiedad intelectual - Datos de salud (RGPD cat. especial) - Estrategia corporativa 5+ anos - Contratos confidenciales Accion: proteger YA con AES-256-GCM
EXPOSICION BAJA	RIESGO BAJO - Documentos operativos cotidianos - Comunicaciones internas breves - Logs y registros de actividad Accion: monitorizar en Fase 3	RIESGO ALTO - Expedientes legales / judiciales - Historiales medicos - I+D y codigo fuente critico - Bases de datos de clientes Accion: inventariar y cifrar en Fase 1

CLASIFICACION POR SECTOR

Sector	Datos en riesgo critico	Urgencia
Asesorias / Gestorias	Expedientes fiscales, datos bancarios clientes	MUY ALTA
Salud / Clinicas	Historiales medicos, datos biometricos	MAXIMA
Legal / Notarias	Expedientes judiciales, escrituras, contratos	MUY ALTA
Tecnologia / SaaS	Codigo fuente, IPs, datos clientes enterprise	ALTA
Industria / I+D	Formulas, patentes, disenos industriales	ALTA
AAPP / Educacion	Datos ciudadanos, expedientes (ENS, NIS2)	MUY ALTA

03 · CRONOGRAMA DE MIGRACION POST-CUANTICA

Plan de accion en tres fases. Cada fase se construye sobre la anterior.

FASE 1 · 2025 — VISIBILIDAD Y FUNDAMENTOS

-> Completar el inventario criptografico de toda la organizacion

-> Actualizar a TLS 1.3 en todos los servidores web y VPN

-> Eliminar algoritmos obsoletos: MD5, SHA-1, DES, RSA < 2048 bits

-> Implementar cifrado de archivos sensibles con AES-256-GCM

-> Empezar formacion del equipo tecnico en post-cuantica

-> Identificar proveedores con dependencias criptograficas criticas

FASE 2 · 2026 — PRIMERAS IMPLEMENTACIONES PQC

-> Migrar TLS a modo hibrido (clasico + ML-KEM simultaneamente)

-> Actualizar PKI interna para soportar ML-DSA (firmas post-cuanticas)

-> Implementar ML-KEM en sistemas de intercambio de claves criticos

-> Migrar VPN y acceso remoto a algoritmos post-cuanticos

-> Revisar contratos con proveedores: anadir clausulas PQC

-> Auditoria externa del estado de la migracion

FASE 3 · 2027+ — CONSOLIDACION Y CERTIFICACION

-> Completar migracion de sistemas legacy pendientes

-> Renovar todos los certificados digitales con algoritmos PQC

-> Validar cumplimiento con ENS actualizado y NIS2

-> Establecer ciclos de auditoria criptografica anuales

-> Implementar agilidad criptografica como politica permanente

-> Certificacion formal de la migracion completada

5 ACCIONES QUE PUEDES HACER ESTA SEMANA

[+] 1. Cambia el DNS de tu red a Quad9 (9.9.9.9) -- 5 minutos, gratis

[+] 2. Activa TLS 1.3 en tu servidor web -- comprueba con testssl.sh

[+] 3. Cifra tus archivos mas sensibles con AES-256-GCM (ChacalCrypt)

[+] 4. Haz una lista de datos con vida util > 10 anos en tu organizacion

[+] 5. Lee los estandares NIST FIPS 203/204/205 o mi libro en Amazon