TECNODATA

Solución Integral de Ciberseguridad y Resiliencia

Prevenir · Contener · Recuperar · **Ver**

Con Halcyon Anti-Ransomware y BlueCat Network Observability

Ciudad de México · Julio 2026 · Documento confidencial

La amenaza ya cambió. Las defensas tradicionales, no.

58%

de los ataques entra por correo electrónico: la puerta principal sigue siendo el buzón de sus empleados.

98%

de las víctimas de ransomware ya tenía un antivirus avanzado (EDR). Lo evadieron de todas formas.

69%

de los ataques ocurre de noche o en fin de semana, cuando nadie está mirando.

Y lo más grave: el robo de información ocurre semanas antes del cifrado, sin que nadie lo detecte. Cuando aparece la nota de rescate, el daño ya está hecho.

¿Qué está realmente en juego?

Un solo incidente exitoso no es un problema de TI. Es un problema institucional.

Continuidad operativa

Semanas sin sistemas: sin operación, sin atención, sin ingresos.

Cumplimiento regulatorio

Sanciones y observaciones de CNBV y del OIC por datos personales comprometidos.

Costo financiero directo

Rescate, recuperación forense, servicios legales y gastos extraordinarios.

Confianza y reputación

El daño reputacional con clientes, fondeadores y autoridades no se restaura en horas.

La pregunta correcta no es “¿cuánto cuesta protegerse?”, sino “¿cuánto cuesta no hacerlo?”

Nuestra respuesta: un modelo de resiliencia total

Cuatro etapas que cubren todo el ciclo de defensa, desplegables por fases y alineadas a NIST y CNBV.

1

PREVENIR

Cerrar la puerta de entrada: correo con IA y accesos sin contraseña.

2

CONTENER

Detectar y aislar lo que logre entrar. Halcyon neutraliza el ransomware en ejecución.

3

RECUPERAR

Respaldos que el ransomware no puede tocar. Operación restaurada en horas, sin pagar rescate.

4

VER

Visibilidad total de la red con BlueCat: no se puede proteger lo que no se ve.

Todo vigilado 24/7/365 desde un SOC operado en México: sus datos nunca salen del país.

Siete componentes, una sola defensa

1 · Protección de correo

Bloquea el correo malicioso con IA (Abnormal AI), la vía de entrada #1.

2 · Accesos sin contraseña

Elimina el robo de credenciales: biometría, SSO y control de privilegios.

3 · Contención y anti-ransomware

Halcyon + Sophos XDR + Firewall: detecta, aísla y neutraliza el ataque.

4 · Vulnerabilidades y DevSecOps

Encuentra y corrige fallas antes de que el atacante las aproveche (GitLab).

5 · Resiliencia de datos

Respaldos inmutables de sistemas, M365 y Active Directory. Recuperación en horas.

6 · SOC 24/7 en México

Vigilancia y respuesta 365 días, con soberanía de datos (KIO Networks).

7 · Observabilidad de red

BlueCat: visibilidad total del tráfico para diagnosticar y anticipar fallas.

MÓDULO 1 · ABNORMAL AI

Protección de correo: cerrar la puerta principal

El 91% de las brechas empresariales comienza con un correo. Abnormal AI aprende cómo se comunica normalmente cada empleado y proveedor, y detiene lo que no encaja: fraudes, suplantaciones y phishing que los filtros tradicionales dejan pasar.

IA que entiende el contexto

Analiza más de 40,000 señales de comportamiento para detectar la intención del atacante, no solo palabras clave.

Sin tocar su operación

Se integra a Microsoft 365 en 3 clics, en modo solo lectura. No retrasa ningún correo ni requiere cambios de red.

Limpia solo, en segundos

Retira automáticamente los correos maliciosos del buzón y desactiva cuentas comprometidas sin intervención manual.

Resultados comprobados: 4× menos correos maliciosos en las bandejas, 92% menos falsas alarmas y más de 15 horas semanales recuperadas por el equipo de seguridad.

2× Líder en el Cuadrante Mágico de Gartner (2025) · Líder en Forrester Wave 2025 · 4,500+ clientes.

MÓDULO 2 · PASSWORDLESS · SSO · PAM

Accesos sin contraseña: nada que robar

El 81% de las brechas involucra contraseñas robadas. La solución es simple: eliminarlas. Cada persona accede con su huella o su dispositivo, y solo a lo que necesita.

Autenticación biométrica

Sin contraseña que adivinar, robar o pescar por phishing. El acceso es la persona, no un texto.

Un solo acceso a todo (SSO)

Un punto de entrada seguro a todos los sistemas: menos puertas, menos riesgo, menos fricción para el usuario.

Control de cuentas privilegiadas

Los administradores de servidores y bases de datos operan bajo vigilancia: cada sesión queda grabada para auditoría del OIC.

Detección de cuentas anómalas

Vigilancia continua de Active Directory: usuarios, permisos y comportamientos fuera de lo normal se alertan en tiempo real.

Compatible con su infraestructura actual (Active Directory, M365, VPN) y con trazabilidad completa para reportes CNBV.

MÓDULO 3 · HALCYON ANTI-RANSOMWARE

El 20% que evade al antivirus es el 100% del daño

Su EDR detecta muy bien. Halcyon cubre lo que ningún EDR cubre solo: el momento exacto en que el ransomware empieza a cifrar. Es la caja fuerte con cerrojo.

Captura las llaves de cifrado

Única plataforma que intercepta las llaves del ransomware y descifra los datos afectados automáticamente.

Recuperación sin pagar rescate

Detecta el patrón de cifrado en segundos y revierte el daño. La extorsión pierde su poder.

Validado de forma independiente

Probado por Omdia frente a LockBit 5.0, Akira y técnicas que evaden al EDR clásico.

En resumen: Halcyon convierte la ciberseguridad en una garantía de continuidad operativa, respaldada por expertos del fabricante con descifradores personalizados.

Tecnodata es el socio exclusivo de Halcyon en México.

MÓDULO 6 · KIO NETWORKS · MÉXICO

SOC 24/7/365: alguien siempre está mirando

El 69% de los ataques ocurre de noche o en fin de semana. Un Centro de Operaciones de Seguridad en territorio nacional vigila los siete componentes sin descanso: sus datos nunca salen del país.

Respuesta en 15 minutos

SLA de atención inicial para incidentes críticos, con contención activa y playbooks alineados a Banxico y NIST.

Cacería proactiva de amenazas

Nivel Platinum: analistas que investigan a los grupos criminales que atacan al sector financiero mexicano, antes de que actúen.

Certificaciones grado CNBV

ISO 27001, SOC 1 y SOC 2 Tipo 2, y CERT Carnegie Mellon: las certificaciones que la CNBV exige para tercerizar TI crítico.

Reportes listos para la autoridad

Reporte mensual de amenazas, bitácoras auditables y acceso directo del OIC a los registros de incidentes.

Tres niveles de servicio (Silver · Gold · Platinum) para crecer según sus necesidades, operando desde un centro de datos con seguridad física de grado bancario.

MÓDULO 7 · BLUECAT NETWORK OBSERVABILITY

No se puede proteger lo que no se ve

Cuando algo falla, todos culpan a la red y nadie tiene evidencia. BlueCat le da a su equipo el mapa completo: sucursales, nube, centro de datos y usuarios remotos en una sola vista.

Visibilidad total

Elimina puntos ciegos en toda la red: se acaba la “sala de crisis” y los señalamientos.

LiveAssist: ingeniero de IA

Su equipo pregunta en lenguaje natural y obtiene el diagnóstico de un experto, 24/7.

Fallas resueltas 2× más rápido

Causa raíz automatizada: menos horas de interrupción, menos impacto al negocio.

Seguridad y cumplimiento

Detecta anomalías en el tráfico y conserva la evidencia que piden los auditores.

Líder en GigaOm Radar de Observabilidad de Red · 1,200+ clientes en 100+ países, incluidos sectores financiero y gobierno.