WHITEPAPER · SEGURIDAD OFENSIVA

Red Team

Probar la defensa como lo haría un adversario real.

Cómo las organizaciones en México pasan de suponer que sus controles funcionan a demostrarlo: emulación de adversarios con objetivos de negocio, evidencia de qué se detecta, qué se detiene y qué queda expuesto ante auditores, reguladores y consejo.

324 mil M
intentos de ciberataque en México en 2024 (Fortinet, citado por la ATDT)

MITRE ATT&CK
marco al que mapeamos cada táctica del ejercicio

< 24 h
plazo para reportar incidentes críticos al CSIRT Nacional-APF

25+ años
de QMA operando ciberseguridad para sectores regulados

RESUMEN EJECUTIVO

Por qué Red Team, y por qué ahora

01

El estándar de seguridad en México acaba de subir. La Política General de Ciberseguridad para la Administración Pública Federal es obligatoria desde diciembre de 2025 y su onda de choque alcanza a proveedores del Estado, sector financiero e infraestructura crítica. Reportar un incidente crítico en menos de 24 horas deja de ser una buena práctica para volverse una obligación con consecuencias. La pregunta ya no es si la organización tiene controles, sino si esos controles **resisten a un adversario real** y si el equipo los ve a tiempo.

La mayoría de los programas de seguridad se evalúan contra una lista: ¿existe el control? ¿está documentado? Esa fotografía no responde la pregunta que importa al consejo y al regulador: **si alguien intentara entrar hoy, ¿qué pasaría?** Un Red Team responde esa pregunta con hechos, no con suposiciones.

QMA Red Team emula las tácticas, técnicas y procedimientos de los adversarios relevantes para su sector, con objetivos de negocio acordados y bajo reglas de enfrentamiento estrictas. No buscamos una lista de hallazgos: buscamos demostrar, extremo a extremo, qué se detecta, qué se detiene y cuánto tardaría su equipo en responder. El resultado es evidencia accionable para dirección, para el área técnica y para quien tenga que rendir cuentas ante un auditor.

PANORAMA

El adversario ya no toca la puerta

02

El atacante moderno no fuerza la entrada: usa credenciales válidas, abusa de configuraciones y se mueve lateralmente sin disparar una sola alarma. Probar la defensa exige pensar y operar como él.

El perímetro dejó de existir

Identidades, nube, terceros y trabajo remoto disolvieron el perímetro tradicional. El acceso inicial rara vez es una hazaña técnica: es un correo bien hecho, una credencial filtrada o un servicio expuesto. Una vez dentro, lo que decide el impacto es la detección y la respuesta, no el firewall.

México es objetivo, no espectador

México es un objetivo prioritario para el cibercrimen en la región: el ransomware y el fraude dirigido al sector financiero operan a escala industrial, y las organizaciones más visibles e infraestructuras críticas concentran los ataques de mayor impacto. El costo de descubrir una brecha en producción —y no en un ejercicio controlado— es inmediato y medible.

PANORAMA

Pentest, Red Team y la confusión que cuesta caro

03

No todo ejercicio ofensivo es lo mismo, y contratar el equivocado deja brechas abiertas. Un **análisis de vulnerabilidades** inventaría debilidades conocidas. Una **prueba de penetración** verifica, con alcance acotado, que esas debilidades son explotables. Un **Red Team** va más allá: persigue un objetivo de negocio —acceder a datos de tarjeta, mover una transferencia, llegar al entorno de respaldo— emulando a un adversario real y **poniendo a prueba a las personas, los procesos y la tecnología a la vez**.

La diferencia es el objetivo, no la herramienta

El pentest pregunta «¿se puede explotar esto?». El Red Team pregunta «¿puede un adversario lograr su objetivo sin que lo veamos?». Por eso el Red Team incluye, cuando el alcance lo permite, ingeniería social, evasión de detección y movimiento lateral sostenido en el tiempo. Es la prueba más cercana a un incidente real sin sufrir uno.

Assume breach: empezar desde dentro

Cuando el objetivo es medir detección y respuesta, partimos del supuesto de que el adversario ya entró (assume breach). Así el ejercicio no se agota intentando cruzar la puerta: mide lo que de verdad contiene el daño —la capacidad de detectar, contener y expulsar— que es justo lo que un regulador espera ver funcionando.

EL ENFOQUE

Emulación con objetivos de negocio 04

Inteligencia primero, no fuerza bruta

Diseñamos cada ejercicio a partir de los adversarios que realmente amenazan a su sector y de los activos cuyo compromiso dolería de verdad. Las técnicas se mapean a **MITRE ATT&CK**, de modo que cada acción del ejercicio queda trazada a una táctica reconocida y su resultado puede compararse contra su capacidad de detección, control por control.

Reglas de enfrentamiento estrictas

Operamos bajo reglas de enfrentamiento (ROE) acordadas y autorización por escrito. Definimos qué está dentro y fuera de alcance, ventanas de operación, criterios de parada y un canal directo para abortar. El objetivo es **probar la defensa sin poner en riesgo la operación**: ningún ejercicio vale una interrupción no planeada de su negocio.

Una sola disciplina, varios marcos satisfechos

El mismo ejercicio que evidencia su postura ofensiva alimenta su programa de cumplimiento: aporta a los requisitos de pruebas de seguridad de ISO/IEC 27001, PCI DSS y la Política APF, y se alinea con NIST SP 800-115 y el marco PTES. Preparar bien una prueba adelanta a las demás: la evidencia que produce sirve al auditor, al regulador y al consejo.

CAPACIDADES

Qué probamos

05

EXTERNO | INTERNO | WEB / APP | INGENIERÍA SOCIAL | NUBE | OT / ICS

Perímetro externo

Lo que un adversario ve desde Internet: servicios expuestos, credenciales filtradas y superficie de ataque real.

Alcance: activos públicos, VPN, correo, portales y exposición en fuentes abiertas.

Entregable: mapa de superficie de ataque y rutas de acceso inicial viables.

Red interna

Qué pasa una vez dentro: escalamiento de privilegios y movimiento lateral hasta los activos críticos.

Alcance: Active Directory, segmentación, rutas a datos y a respaldo.

Entregable: cadena de compromiso documentada hasta el objetivo de negocio.

Aplicaciones y APIs

Las puertas que su negocio expone a clientes y socios, probadas contra abuso lógico, no solo técnico.

Alcance: web, APIs y portales transaccionales, alineado a OWASP.

Entregable: hallazgos priorizados por impacto de negocio con prueba de concepto.

Ingeniería social

El vector que abre la mayoría de los incidentes: personas y procesos bajo presión realista y ética.

Alcance: phishing dirigido, pretexting y, si aplica, acceso físico.

Entregable: tasa de exposición y puntos de mejora en concientización y proceso.

Nube e identidad

Configuraciones, identidades y permisos en la nube donde hoy vive el dato y el riesgo.

Alcance: AWS / Azure / M365: identidad, permisos y exposición de cargas.

Entregable: rutas de abuso de identidad y recomendaciones de endurecimiento.

Detección y respuesta

La prueba que más le importa al regulador: ¿lo vemos, lo contenemos y respondemos a tiempo?

Alcance: ejercicio purple team con su SOC y telemetría existente.

Entregable: mapa de cobertura de detección sobre MITRE ATT&CK y tiempos de respuesta.

FOCO

Banca y Fintech: resiliencia que el regulador entiende

06

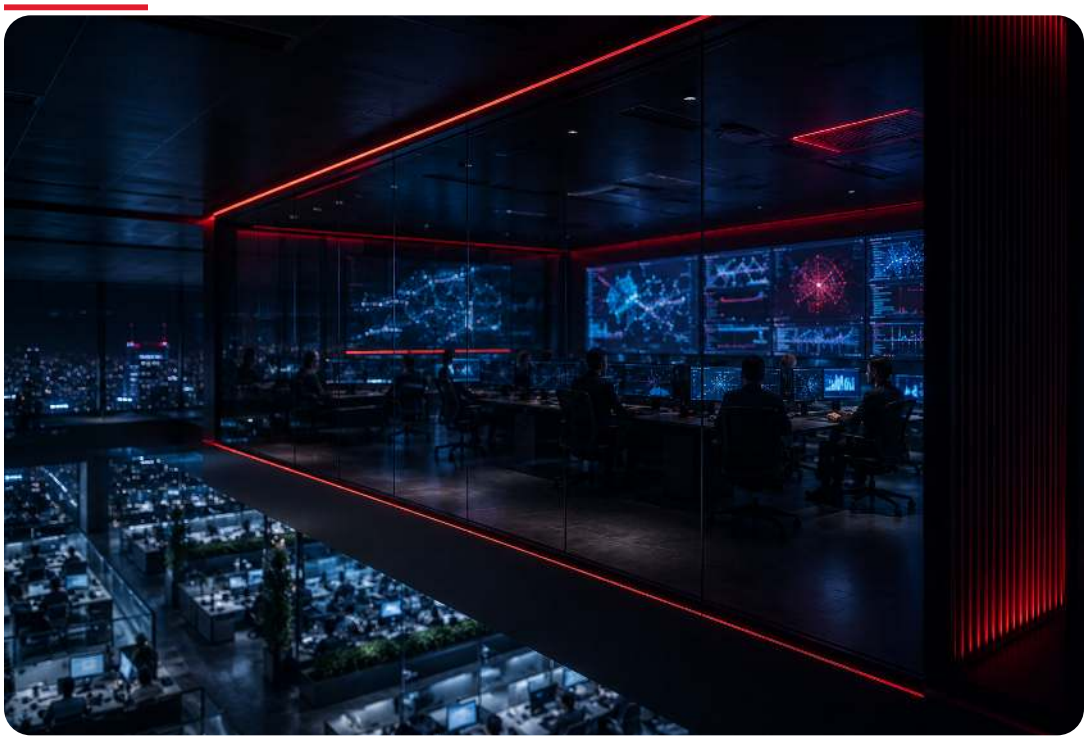
Para una institución financiera o una fintech regulada por la CNBV, demostrar resiliencia operativa dejó de ser opcional: es condición para operar, para cerrar contratos y para sostener la confianza del mercado.

Del control en papel al control que aguanta

Las obligaciones del sector exigen pruebas de seguridad periódicas y capacidad demostrable de detección y respuesta. Un Red Team con objetivos alineados a sus procesos críticos —pagos, transferencias, datos de tarjeta— produce la evidencia que el regulador, el auditor y el consejo necesitan ver: **no que el control existe, sino que funciona bajo presión**.

El costo de descubrirlo en producción

Un fraude consumado, un dato de tarjeta expuesto o un servicio crítico detenido cuestan mucho más —en multa, en reputación y en negocio perdido— que el ejercicio controlado que los habría anticipado. El Red Team convierte un riesgo invisible en una lista priorizada de cosas que arreglar antes de que lo haga un atacante.



METODOLOGÍA

Cómo trabaja un ejercicio QMA Red Team

07

01 Alcance y reglas de enfrentamiento

Definimos objetivos de negocio, activos dentro y fuera de alcance, ventanas, criterios de parada y autorización por escrito. Nada empieza sin ROE firmadas.

02 Inteligencia y modelado de amenaza

Perfilamos a los adversarios relevantes para su sector y mapeamos sus TTP a MITRE ATT&CK para diseñar un ejercicio creíble, no genérico.

03 Emulación y acceso

Reproducimos las técnicas del adversario para obtener acceso, de forma controlada y trazable. Todo queda registrado para reconstruir la cadena después.

04 Movimiento hacia el objetivo

Escalamos privilegios y nos movemos hacia el activo objetivo, midiendo en cada paso qué detecta y qué deja pasar su defensa.

05 Reporte ejecutivo y técnico

Dos lecturas del mismo ejercicio: un resumen para dirección con riesgo de negocio y prioridades, y un detalle técnico reproducible para el equipo, con evidencia.

06 Remediación y retest

Acompañamos el cierre de brechas y validamos con un retest que lo corregido quedó efectivamente cerrado. La mejora se demuestra, no se asume.

QUIÉNES SOMOS

QMA

QMA es una empresa mexicana de ciberseguridad con más de 25 años de operación continua (constituida en el año 2000), especializada en servicios administrados de seguridad para sectores regulados. Operamos seguridad ofensiva y defensiva bajo una misma disciplina de evidencia.

Lleve su defensa de la suposición a la evidencia

El adversario no espera a su próxima auditoría. Empecemos por un scoping: qué objetivos probar, bajo qué reglas y qué evidencia necesita para dirección, regulador y consejo. Sin compromiso y con reglas de enfrentamiento claras desde el primer día.

Solicite un scoping de Red Team

qma.mx · +52 55 5341 6928 · soporte@qma.mx