WHITEPAPER · SEGURIDAD OFENSIVA

Pentesting

Verificar, con evidencia, qué tan lejos llega un atacante.

No opina sobre su seguridad: la demuestra. Verificamos qué es realmente explotable, con qué impacto de negocio y cómo cerrarlo — con método reconocido.

3 enfoques
caja negra, gris y blanca según objetivo y nivel de acceso acordado

PCI DSS 4.0
exige pruebas de penetración periódicas y tras cambios relevantes

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

25+ años
de QMA probando sistemas en sectores regulados

RESUMEN EJECUTIVO

Probar no es opinar: es demostrar

01

Cumplir una lista de controles no responde la pregunta que importa: ¿esos controles aguantan un intento real? Una prueba de penetración cierra esa brecha. Bajo un alcance acordado y reglas claras, un equipo especializado intenta comprometer sus sistemas como lo haría un atacante, y documenta exactamente **qué funcionó, qué no y por qué**.

El estándar en México ya lo exige de hecho. La Política General de Ciberseguridad para la Administración Pública Federal, obligatoria desde diciembre de 2025, y marcos como PCI DSS e ISO/IEC 27001 piden pruebas de seguridad periódicas y evidencia de que las debilidades se corrigen. Una prueba bien hecha satisface varias de esas exigencias con un solo ejercicio.

QMA entrega dos lecturas del mismo trabajo: un resumen ejecutivo con el riesgo de negocio y las prioridades, y un detalle técnico reproducible para que su equipo remedie con precisión. No buscamos asustar con una lista interminable de hallazgos: buscamos que cada hallazgo sea verificable, priorizado y accionable.

PANORAMA

Una debilidad conocida no es lo mismo que una explotable

02

Un escáner produce cientos de alertas; pocas importan de verdad. El valor de una prueba de penetración es separar el ruido de lo que un atacante usaría hoy.

Del inventario a la prueba

Un análisis de vulnerabilidades inventaría debilidades conocidas; es amplio y continuo. La prueba de penetración toma ese inventario y verifica, con alcance acotado, cuáles son realmente explotables y a qué dan acceso. Las dos disciplinas se complementan: una vigila el terreno, la otra confirma el peligro.

El costo de no saberlo a tiempo

Descubrir una ruta de compromiso en producción —un fraude, una fuga de datos, un servicio detenido— cuesta mucho más que el ejercicio controlado que la habría anticipado. La prueba convierte una incertidumbre en una lista corta y priorizada de cosas que arreglar antes de que las encuentre alguien más.

TIPOS DE PRUEBA

El alcance correcto para la pregunta correcta

03

No toda prueba responde lo mismo. Elegir el enfoque adecuado evita pagar de más y, sobre todo, evita dejar fuera lo que importa. QMA define el alcance con usted antes de tocar un solo sistema.

Caja negra, gris y blanca

En **caja negra** partimos sin información, como un atacante externo. En **caja gris** trabajamos con acceso limitado —una cuenta de usuario, documentación parcial— para simular a un insider o a un atacante que ya logró un punto de apoyo. En **caja blanca** revisamos con visibilidad total para máxima cobertura. El enfoque se elige por objetivo, no por moda.

Externo, interno y por activo

Probamos el perímetro expuesto a Internet, la red interna una vez dentro, y activos específicos: aplicaciones web y APIs, infraestructura, redes inalámbricas y entornos en la nube. El alcance se documenta por escrito y nada queda sujeto a interpretación el día del ejercicio.

EL ENFOQUE

Método reconocido, evidencia reproducible

04

Un marco, no una improvisación

Trabajamos sobre marcos reconocidos —**NIST SP 800-115**, **PTES** y, para aplicaciones, la **OWASP** Testing Guide— de modo que el ejercicio sea repetible y comparable en el tiempo. Cada hallazgo se documenta con su evidencia, su impacto y los pasos para reproducirlo en un entorno controlado, **sin publicar nada que sirva de receta a un atacante**.

Reglas de enfrentamiento estrictas

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

Una prueba, varios marcos satisfechos

La misma prueba alimenta su programa de cumplimiento: aporta evidencia para ISO/IEC 27001, PCI DSS y la Política APF, y produce un informe que el auditor, el regulador y el consejo pueden leer. Preparar bien una prueba adelanta el trabajo de las demás.

CAPACIDADES

Qué evaluamos

05

EXTERNO | INTERNO | WEB / API | MÓVIL | NUBE | WI-FI / OT

Perímetro externo

Lo que un atacante alcanza desde Internet: servicios expuestos, configuraciones débiles y superficie de ataque real.

Qué prueba: activos públicos, VPN, correo y portales expuestos.

Resultado: rutas de acceso inicial viables, priorizadas por riesgo.

Red interna

Qué pasa una vez dentro: escalamiento de privilegios y alcance hacia los activos críticos del negocio.

Qué prueba: segmentación, Active Directory y rutas a datos sensibles.

Resultado: cadena de compromiso documentada y puntos de corte.

Aplicaciones y APIs

Las puertas que su negocio expone a clientes y socios, probadas contra abuso técnico y de lógica de negocio.

Qué prueba: web, APIs y portales transaccionales, alineado a OWASP.

Resultado: hallazgos con prueba de concepto e impacto de negocio.

Aplicaciones móviles

El canal que más crece en banca y retail: la app y su comunicación con el back-end, de extremo a extremo.

Qué prueba: cliente móvil, almacenamiento local y APIs asociadas.

Resultado: exposición de datos y abuso de funciones, priorizado.

Nube e identidad

Configuraciones, identidades y permisos en la nube, donde hoy vive buena parte del dato y del riesgo.

Qué prueba: AWS / Azure / M365: permisos, exposición y postura.

Resultado: configuraciones de riesgo y recomendaciones de endurecimiento.

Inalámbrico y OT

Redes Wi-Fi corporativas y, cuando aplica, entornos industriales que rara vez se prueban y casi siempre exponen.

Qué prueba: Wi-Fi, segmentación y acceso a entornos OT / ICS.

Resultado: puntos de entrada al entorno corporativo e industrial.

FOCO

PCI DSS y banca: la prueba que el estándar exige

06

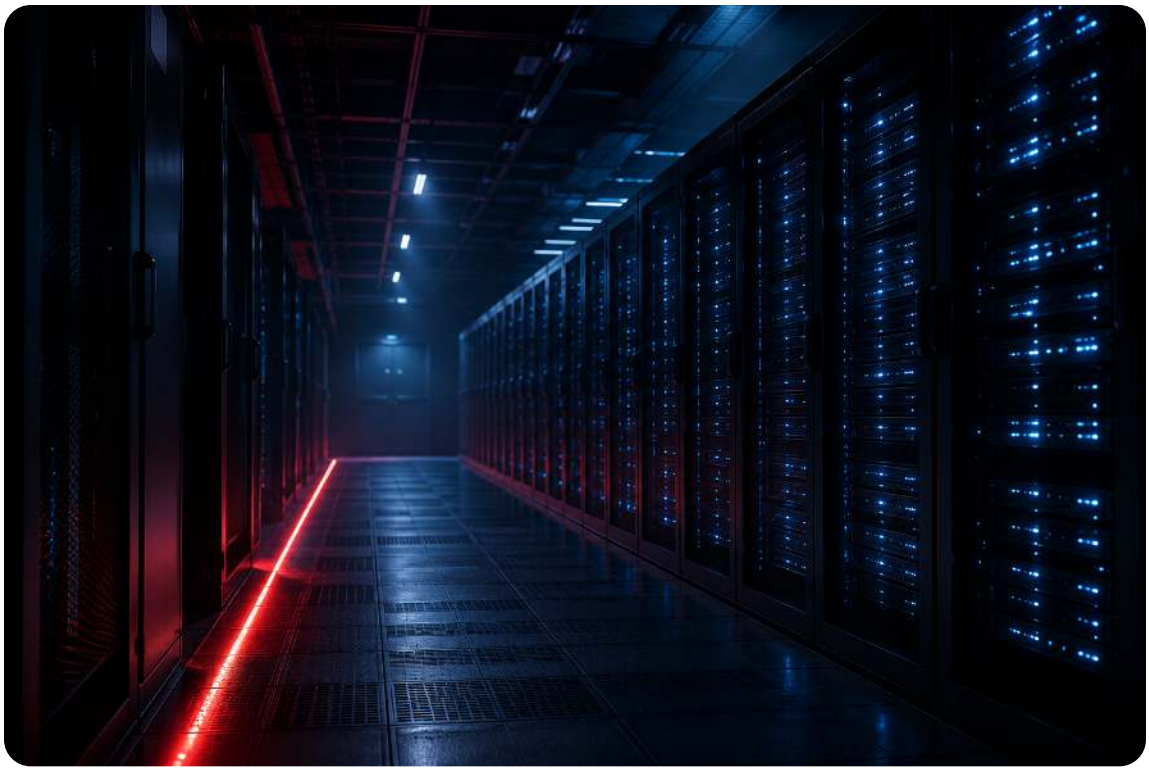
Para quien procesa pagos o datos de tarjeta, la prueba de penetración no es una buena práctica opcional: es un requisito explícito del estándar y una condición para operar y cerrar contratos.

Cumplir con evidencia, no con un PDF genérico

PCI DSS exige pruebas de penetración periódicas y tras cambios significativos, sobre el entorno de datos de tarjeta y su segmentación. Una prueba con alcance bien definido produce justo lo que el evaluador (QSA) necesita ver: **que el control existe y que funciona bajo presión**, no solo que está documentado.

Segmentación: lo que de verdad reduce el alcance

Validar que la segmentación aísla el entorno de tarjeta del resto de la red puede reducir drásticamente el alcance —y el costo— de su cumplimiento. Es uno de los ejercicios con mejor retorno para una institución financiera o una fintech regulada por la CNBV.



METODOLOGÍA

Cómo trabaja una prueba QMA

07

01 Alcance y reglas de enfrentamiento

Acordamos objetivos, activos dentro y fuera de alcance, enfoque (negra/gris/blanca), ventanas, criterios de parada y autorización por escrito. Nada empieza sin ROE firmadas.

02 Reconocimiento y mapeo

Levantamos la superficie real de los activos en alcance y la mapeamos, para enfocar el esfuerzo donde el riesgo es mayor y no desperdiciar la ventana de prueba.

03 Identificación de debilidades

Combinamos herramienta y análisis manual para separar el ruido del escáner de las debilidades que un atacante usaría de verdad.

04 Verificación controlada

Confirmamos la explotabilidad de forma controlada y trazable, midiendo el impacto real sin afectar la operación. Todo queda registrado para reconstruirlo después.

05 Reporte ejecutivo y técnico

Dos lecturas del mismo trabajo: un resumen para dirección con riesgo y prioridades, y un detalle técnico reproducible para el equipo, con evidencia y remediación sugerida.

06 Remediación y retest

Acompañamos el cierre 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.

Deje de suponer que sus controles aguantan

Empecemos por un scoping: qué activos probar, bajo qué enfoque y qué evidencia necesita para cumplimiento y para su equipo técnico. Con reglas de enfrentamiento claras desde el primer día y sin riesgo para su operación.

Solicite un scoping de pentest

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