WHITEPAPER · CUMPLIMIENTO GESTIONADO

QMA CERTEZA

Del requisito regulatorio a la evidencia auditable, en continuo.

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

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

~15 jun 2026
plazo de la ATDT para lineamientos técnicos de la Política APF

25+ años
de QMA operando ciberseguridad para sectores regulados

RESUMEN EJECUTIVO

Por qué ahora, y por qué Certeza

01

El estándar de cumplimiento 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 ya alcanza a proveedores del Estado, sector financiero e infraestructura crítica. En paralelo, marcos como SOC 2, ISO 27001 y PCI DSS dejaron de ser un diferenciador para volverse la puerta de entrada a contratos enterprise, a la due diligence de inversionistas y a vender en Estados Unidos.

El problema no es la falta de marcos, sino el modelo con que se cumplen. La auditoría anual produce una fotografía: cierto el día que se toma, desactualizada semanas después. Mientras tanto, el costo de un hallazgo en auditoría, de un deal trabado por no tener SOC 2 o de un incidente no reportado a tiempo es inmediato y medible.

QMA Certeza es la respuesta de QMA a ese desfase: cumplimiento gestionado con evidencia continua. Traducimos las obligaciones —de la Política APF, de los reguladores sectoriales mexicanos y de los marcos internacionales— a controles operativos y a evidencia lista para auditoría, y la mantenemos viva en lugar de reconstruirla una vez al año. Y lo hacemos con la precisión que cada marco exige: QMA prepara y acompaña; la certificación o atestiguación la emite el tercero acreditado correspondiente.

La ventaja del enfoque es estructural: preparar bien un marco adelanta a los demás. Los controles que satisfacen ISO 27001 cubren buena parte de SOC 2; la arquitectura Zero Trust que reduce el alcance de PCI DSS es la misma que pide la Política APF. Una sola disciplina de evidencia, varios marcos satisfechos.

PANORAMA

El cumplimiento en México cambió de nivel

02

Tres fuerzas convergen sobre cualquier organización que opere en México y quiera crecer: la nueva política federal, los reguladores sectoriales y la presión del mercado enterprise e internacional. Las tres empujan en la misma dirección: evidencia, trazabilidad y controles auditables.

La política federal ya es obligatoria

El 17 de diciembre de 2025 la Agencia de Transformación Digital y Telecomunicaciones (ATDT) publicó en el Diario Oficial de la Federación la Política General de Ciberseguridad para la APF, vigente desde el 18 de diciembre. La ciberseguridad dejó de ser guía voluntaria y se volvió obligación administrativa sujeta a auditorías. El plazo de designación de responsables (60 días) ya venció; el de lineamientos técnicos de la ATDT vence a mediados de junio de 2026. La política exige reportar incidentes críticos al CSIRT Nacional-APF en menos de 24 horas y se alinea de forma explícita con ISO/IEC 27001, NIST SP 800-207 (Zero Trust) y CIS Controls.

Los reguladores sectoriales ya sancionan

México ya cuenta con instrumentos con consecuencias económicas reales: la LFPDPPP contempla multas de hasta unos 72 millones de pesos por datos sensibles; la LIC y la Ley Fintech facultan a la CNBV para multar e incluso revocar. Según el análisis de QMA sobre el corpus público de sanciones de la CNBV, las multas acumuladas superan los 3,980 millones de pesos. Nota relevante: el INAI fue disuelto en marzo de 2025 y sus funciones de protección de datos las asumió la Secretaría Anticorrupción y Buen Gobierno; las obligaciones siguen vigentes, cambió la autoridad que las ejecuta.

El mercado exige la prueba antes del contrato

Cada vez más clientes enterprise y fondos de inversión piden SOC 2 o ISO 27001 como condición para firmar o invertir, y la Política APF eleva el estándar para proveedores del gobierno con su eje de cadena de suministro y terceros confiables. Para una empresa mexicana que quiere vender hacia arriba o cruzar la frontera, el cumplimiento dejó de ser un trámite posterior: es el requisito de entrada.

El acelerador: el Mundial 2026

Como sede, México anticipa un aumento significativo de ataques de alto impacto durante el torneo. La urgencia regulatoria y la operativa apuntan al mismo trimestre. Llegar preparado a junio de 2026 no es teoría: es calendario.

LA SOLUCIÓN

Qué es QMA Certeza

03

QMA Certeza es el servicio de cumplimiento gestionado de QMA. Combina nuestra operación de seguridad, una plataforma de automatización de cumplimiento con evidencia continua y una lectura propia de la regulación mexicana, para llevar a una organización del requisito a la evidencia auditable —y mantenerla ahí.

Lectura regulatoria mexicana

Traducimos la Política APF, la regulación CNBV/Banxico, la Ley Fintech y los marcos internacionales a un lenguaje de controles y obligaciones concretas para su sector.

Controles y evidencia continua

Mapeamos cada obligación a un control operativo y a la evidencia que un auditor o regulador espera ver; la evidencia se recolecta y conserva de forma continua, no en una corrida anual.

Preparación para el tercero correcto

Dejamos a la organización lista para el organismo acreditado, el CPA o el QSA que corresponda. QMA no certifica ni atestigua: prepara, acompaña y sostiene.

El resultado es certeza accionable: un tablero de estado por marco, evidencia viva y una posición sólida frente a auditores, reguladores y consejo —sin depender de esfuerzos heroicos cada vez que llega una auditoría o un cliente exigente.

EL ENFOQUE

Integrado, continuo y Zero Trust

04

Preparar una vez, satisfacer varios

Los marcos comparten más controles de los que parece. ISO 27001 e ISO 9001 conviven bajo la estructura común del Anexo SL; SOC 2 reutiliza buena parte de los controles de 27001; NIST CSF 2.0 sirve de crosswalk con todo lo demás. QMA Certeza diseña el programa para que un mismo control —con su evidencia— responda a varios marcos a la vez. Eso reduce el re-trabajo y el costo de oportunidad de prepararse marco por marco.

Evidencia continua, no una fotografía anual

La auditoría tradicional certifica un instante. Nuestro enfoque mantiene la evidencia viva: controles monitoreados, hallazgos remediados y registros disponibles cuando el auditor, el regulador o el cliente los pidan. La diferencia entre demostrar que se cumple hoy y recordar que se cumplía en la última auditoría.

Zero Trust como columna vertebral

La arquitectura Zero Trust —ningún usuario, dispositivo o red confiable por defecto— es a la vez control de seguridad y palanca de cumplimiento. Reduce el alcance del entorno de datos de tarjeta en PCI DSS, satisface el eje de identidad y accesos de la Política APF y se alinea con NIST SP 800-207. Menos superficie, más evidencia, mismo esfuerzo.

POR MARCO

Un recorrido con la precisión correcta

05

Cada marco resuelve un dolor distinto del comprador y exige una precisión distinta. Así acompaña QMA Certeza a cada uno —con el rol de QMA y del tercero siempre claro.

ISO/IEC 27001

Seguridad de la información que sus clientes auditan. La base sobre la que se construye el resto del programa.

Precisión: la certificación la emite un organismo acreditado (EMA); QMA prepara y opera el SGSI.

Encaja con: el enfoque integrado: es el cimiento de SOC 2 y de la Política APF.

ISO 9001

Calidad demostrable sin frenar la operación, con procesos auditables que conviven con la seguridad.

Precisión: la ruta al certificado pasa por un organismo acreditado; QMA prepara el sistema de gestión.

Encaja con: ISO 27001 bajo la estructura común del Anexo SL.

SOC 2

La atestiguación que desbloquea deals enterprise y la venta hacia Estados Unidos.

Precisión: la atestiguación la firma un CPA independiente; QMA prepara y sostiene la evidencia continua, no la foto anual.

Encaja con: ISO 27001: comparten gran parte de los controles.

PCI DSS 4.0.1

Datos de tarjeta sin sobresaltos, con un alcance claro y bajo control.

Precisión: valida un QSA (ROC) o un SAQ con AOC, y escanea un ASV; QMA no es QSA: reduce alcance y prepara.

Encaja con: Zero Trust para encoger el entorno de datos de tarjeta (CDE).

NIST CSF 2.0

Madurez medible que el consejo entiende y que ordena la inversión.

Precisión: es un marco de postura, no una certificación; QMA lo usa como tablero de madurez.

Encaja con: el crosswalk que conecta todos los demás marcos.

Marcos personalizados — REPSE / PLD

Radar regulatorio mexicano convertido en controles auditables y evidencia.

Precisión: fuera del núcleo cyber: QMA entra como capa de seguridad, evidencia y monitoreo, no como asesoría laboral ni legal AML.

Encaja con: la evidencia cruzada del resto del programa.

FOCO

Fintech Starters: cumplir es crecer

06

Para una fintech regulada por la CNBV o bajo la Ley Fintech, el cumplimiento no es un gasto: es la llave del crecimiento. SOC 2, PCI DSS e ISO 27001 son, a la vez, la puerta a contratos enterprise, el requisito de la due diligence de inversionistas y la condición para vender en Estados Unidos.

El costo de oportunidad es real

Un deal enterprise trabado por no tener SOC 2, o una ronda que se enfría porque la due diligence encuentra controles inmaduros, cuestan mucho más que el programa de cumplimiento que los habría evitado.

Preparar una vez, satisfacer a varios

El enfoque integrado de QMA Certeza evita el re-trabajo: los controles que exige el inversionista se reutilizan para el cliente enterprise y para el regulador. No es una promesa de velocidad mágica —es eficiencia de programa, defendible y propia.

El reloj corre a favor de quien se anticipa

Entre el levantamiento de capital y el pipeline enterprise, la fintech que llega con evidencia continua negocia desde la fuerza; la que improvisa, desde la urgencia.

EL MÉTODO

Cinco fases, del diagnóstico a la certeza

07

QMA Certeza opera con un método de cinco fases. La mecánica fina es propietaria; el principio es transparente: del diagnóstico a la evidencia viva, con el tercero acreditado siempre en su lugar.

01 **Diagnóstico y alcance**
Evaluación de readiness y definición de alcance por marco: dónde está la organización, qué exige cada marco y dónde están las brechas.

02 **Mapeo de obligaciones a controles**
Cada obligación regulatoria o de marco se traduce a un control operativo concreto y a la evidencia que lo demuestra.

03 **Cierre de brechas**
Implementación y endurecimiento de controles —apoyados en la operación de seguridad y la arquitectura Zero Trust de QMA— para cerrar lo que el diagnóstico encontró.

04 **Evidencia continua**
Recolección y custodia continua de la evidencia, con un tablero de estado por marco. La postura se mantiene viva, lista para mostrarse.

05 **Atestiguación y mejora continua**
Preparación para el organismo acreditado, el CPA o el QSA correspondiente, y ciclo de mejora continua para sostener el cumplimiento en el tiempo.

QUIÉNES SOMOS

QMA

08

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 y de alta criticidad. Opera seguridad gestionada (SOC/MDR) con equipo propio y una red consolidada de especialistas, con SOC as a Service sobre AWS y Microsoft, y produce inteligencia de amenazas propia con lente de México y Latinoamérica. Es miembro verificado de MSPAlliance bajo el Unified Certification Standard desde 2011, un estándar auditado por terceros.

Lo que nos distingue

Operación con gobierno en México
SOC/MDR con equipo QMA y red de especialistas, con datos y gobierno del servicio en México, y SOC as a Service sobre AWS y Microsoft.

Respaldo de plataformas líderes
Socio certificado de los fabricantes de ciberseguridad líderes del mundo, integrados en una sola operación con un punto de responsabilidad.

Inteligencia propia, lente LATAM
Inteligencia de amenazas producida internamente con contexto de exposición de México y Latinoamérica, sin demoras de traducción.

Certificación independiente
Miembro verificado de MSPAlliance bajo el Unified Certification Standard desde 2011, auditado por terceros.

Precisión de claims
Postura de claims: QMA implementa, prepara y opera los marcos de seguridad y cumplimiento para sus clientes. La certificación o atestiguación la emite, en cada caso, el organismo acreditado, el CPA independiente o el QSA que corresponda.

Lleve a su organización del requisito a la certeza

El plazo de la Política APF, el siguiente deal enterprise y la próxima ronda no esperan. Empecemos por una evaluación de readiness: dónde está su organización, qué marcos abren más valor y cómo llegar con evidencia continua.

Solicite su evaluación de readiness

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