Ecosistema de Ciberseguridad Financiera 2026

Estrategias de Resiliencia, Cumplimiento CNBV y Metodología OWASP

Ulises M. Álvarez

CISO del Poder Ejecutivo del Estado de Querétaro

Guadalajara, México | Junio 2026

AGENDA EJECUTIVA

I. Contexto Normativo

- Marco Regulatorio CNBV (CUB/CUCB)
- Gobernanza y Responsabilidad (Art. 168)
- Gestión de Riesgos y Anexos Técnicos

II. Metodología OWASP

- Análisis de Riesgo en el SDLC
- Cuantificación de Probabilidad e Impacto
- Simulación Práctica: SQL Injection

EL PANORAMA DE AMENAZAS EN MÉXICO

"La ciberseguridad no es un reto tecnológico, sino un riesgo estratégico y de gobernanza sistémica."

GOBERNANZA Y RESPONSABILIDAD (ART. 168)

La Responsabilidad del Mando

El **Artículo 168 Bis 11** de la CUB establece que el Director General es el responsable último de la implementación del Sistema de Control Interno.

- Supervisión directa por el Consejo.
- Estrategia alineada a la viabilidad operativa.
- Eliminación de ambigüedad en la propiedad del riesgo.

ESTRUCTURA DEL OFICIAL DE SEGURIDAD (CISO)

Jerarquía

Debe reportar directamente al Director General para evitar conflictos con unidades de negocio.

Plan Director

Responsable de elaborar el Plan Director de Seguridad con inversiones y cronogramas.

Monitoreo

Vigilancia permanente a través de oficiales operativos en cada unidad de negocio.

LA NUEVA MURALLA ANTIFRAUDE

Anexo 12-E (Junio 2024)

Este anexo introduce lineamientos proactivos para elevar la protección del usuario a prioridad estratégica.

- Detección de fraude en tiempo real (SDF).
- Responsable de Prevención de Fraude (RPF).
- Monto Transaccional del Usuario (MTU).

MTU: REDEFINIENDO LA CARGA DE LA PRUEBA

A partir de **Enero 2026**, todos los clientes deben configurar su Monto Transaccional del Usuario (MTU).

Regla de las 48 Horas

Si una transacción supera el MTU sin 2FA, la institución asume la responsabilidad total y debe reembolsar en un máximo de 48 horas.

- Límite por defecto: 1,500 UDIS.
- Incentivo a biometría y 2FA robusto.
- Mitigación de fraude masivo digital.

GESTIÓN DE TERCEROS Y NUBE (ANEXO 52)

Redundancia

Mecanismos alternos de comunicación y soporte técnico disponible 24/7/365.

Soberanía de Datos

Cifrado punto a punto y custodia de bitácoras en territorio nacional mexicano.

Auditoría Directa

Cláusulas contractuales que permiten a la CNBV inspeccionar físicamente al proveedor.

MODELO DE RESPONSABILIDAD EN LA NUBE

Componente	Responsabilidad del Proveedor (CSP)	Responsabilidad de la Institución
Infraestructura Física	✓Total	—Nula
Aplicaciones y Datos	—Nula	✓Absoluta
Cumplimiento CNBV	Soporte y Auditoría	Due Diligence y Reporte

*Basado en los artículos 318 y 328 de la CUB.

RESPUESTA A CRISIS: LA REGLA DE ORO

60 MIN

El Plazo de Notificación

Ante un incidente grave (interrupción, robo de datos o daño reputacional), la CNBV debe ser notificada en un plazo no mayor a 60 minutos.

CICLO DE REPORTE DE INCIDENTES

60 Minutos

Notificación inicial a la CNBV (CUB Art. 168 Bis 16).

48 Horas

Notificación a clientes afectados si hay pérdida de datos.

5 Días

Entrega de informe técnico (Anexos 64 y 64 Bis).

15 Días

Plan de trabajo para remediación de fallas.

ESPECIFICIDADES DEL SECTOR BURSÁTIL (CUCB)

Artículo 68 y el Control de Órdenes

Filtros automáticos para monitorear órdenes de valores enviadas por medios electrónicos. Prevención de errores operativos que pongan en riesgo la estabilidad del mercado.

Anexo 18

Plan de Continuidad de Negocio (BCP) probado anualmente con enfoque en liquidación y depósito.

Anexo 19

Reportes de eventos de pérdida o acceso no autorizado a información bursátil sensible.

METODOLOGÍA DE ANÁLISIS DE RIESGO

OWASP RR

Un marco estandarizado para traducir debilidades técnicas en prioridades de negocio alineadas con la gobernanza financiera.

OWASP VS. CVSS: ¿POR QUÉ ADOPTARLO?

CVSS (Técnico)

Mide la severidad intrínseca de la vulnerabilidad en el vacío.

Ignora al agente de amenaza y el impacto directo al negocio.

OWASP (Riesgo Real)

Evalúa el **Escenario Completo**.

- Perfil del atacante (habilidad, motivo).
- Facilidad de descubrimiento.
- Impacto financiero y reputacional.

LAS 5 FASES DE LA METODOLOGÍA

1. ID del Riesgo

Identificar vector de ataque y vulnerabilidad.

2. Probabilidad

Facilidad de descubrimiento y explotación.

3. Impacto

Efectos técnicos y daños de negocio.

4. Severidad

Cálculo matricial del riesgo final.

5. Priorización

Orden de atención y remediación.

PROBABILIDAD: FACTORES DEL AGENTE

Factor	Criterio (0-9)	Puntos
Skill Level	Habilidades básicas (3) -> Avanzado (9)	?
Motive	Baja recompensa (1) -> Alta recompensa (9)	?
Opportunity	Acceso físico (0) -> Sin acceso previo (9)	?
Size	Internos (2) -> Usuarios anónimos (9)	?

PROBABILIDAD: FACTORES DE LA VULN.

Facilidad de Descubrimiento

Desde identificación manual compleja (3) hasta herramientas automáticas públicas (9).

Detección de Intrusiones

WAF con bloqueo activo (1) hasta ausencia total de registros o logs (9).

Awareness (Conocimiento)

- Día Cero: 1 punto
- Conocido en círculo cerrado: 4 puntos
- Debilidad obvia de diseño: 6 puntos
- Conocimiento público masivo: 9 puntos

IMPACTO: FACTORES TÉCNICOS

Confidencialidad

Revelación mínima (2) vs Exfiltración masiva de datos críticos (9).

Integridad

Corrupción mínima (1) vs Pérdida total de base de datos (9).

Disponibilidad

Caída temporal de servicios secundarios (1) vs Caída total persistente (9).

Auditabilidad (Responsabilidad)

Rastreable y atribuible (1) vs Anonimato absoluto sin atribución (9).

IMPACTO: FACTORES DE NEGOCIO

Daño Financiero

Costo de corrección (1) vs Daño catastrófico a la viabilidad (9).

Cumplimiento Regulatorio

Violación de política interna (2) vs Sanciones administrativas graves (7).

Daño a la Reputación

Pérdida de cuentas clave (4) vs Daño severo irreversible a la marca (9).

Privacidad

Exposición de un individuo (3) vs Exposición masiva de miles de usuarios (7).

EL CÁLCULO CUANTITATIVO

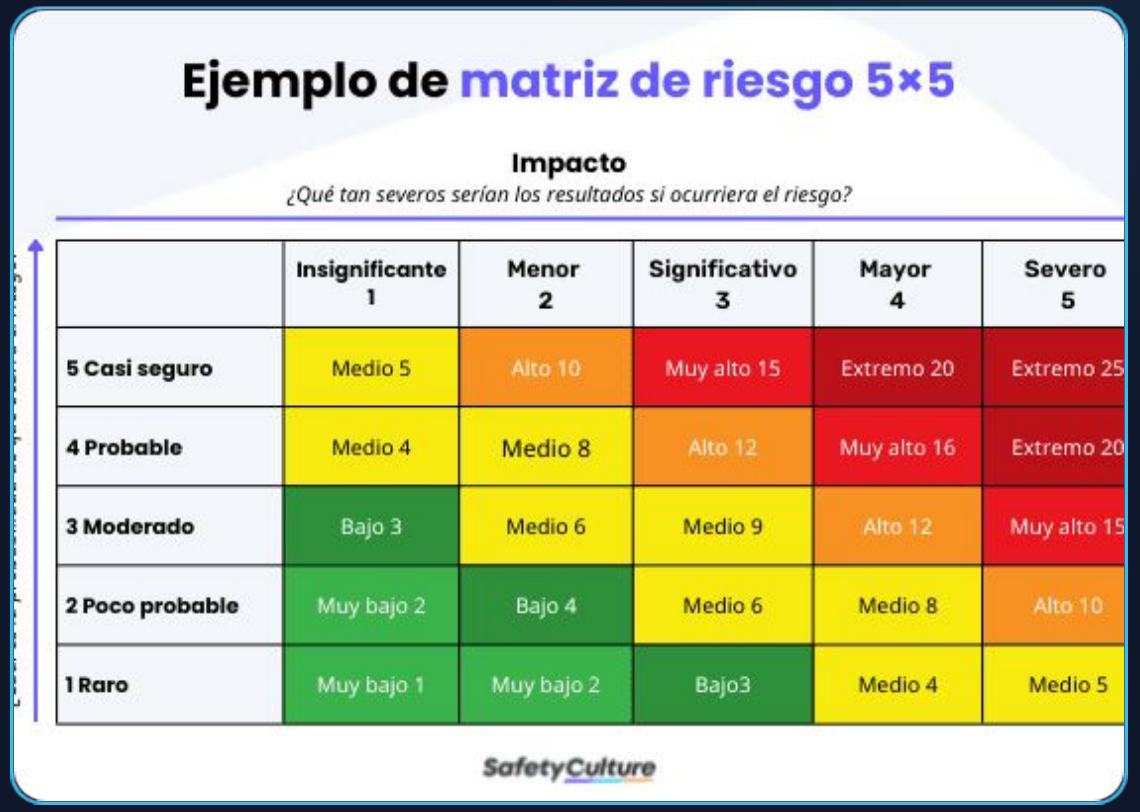
$$P = \frac{\sum FA + \sum FV}{8}$$

$$I = \frac{\sum IT + \sum IB}{8}$$

Bajo	Medio	Alto
0 - 3	3 - 6	6 - 9

MATRIZ DE SEVERIDAD DE RIESGO

Prob \ Imp	BAJO	MEDIO	ALTO
BAJO	Informativo	Bajo	Medio
MEDIO	Bajo	Medio	Alto
ALTO	Medio	Alto	**CRÍTICO**



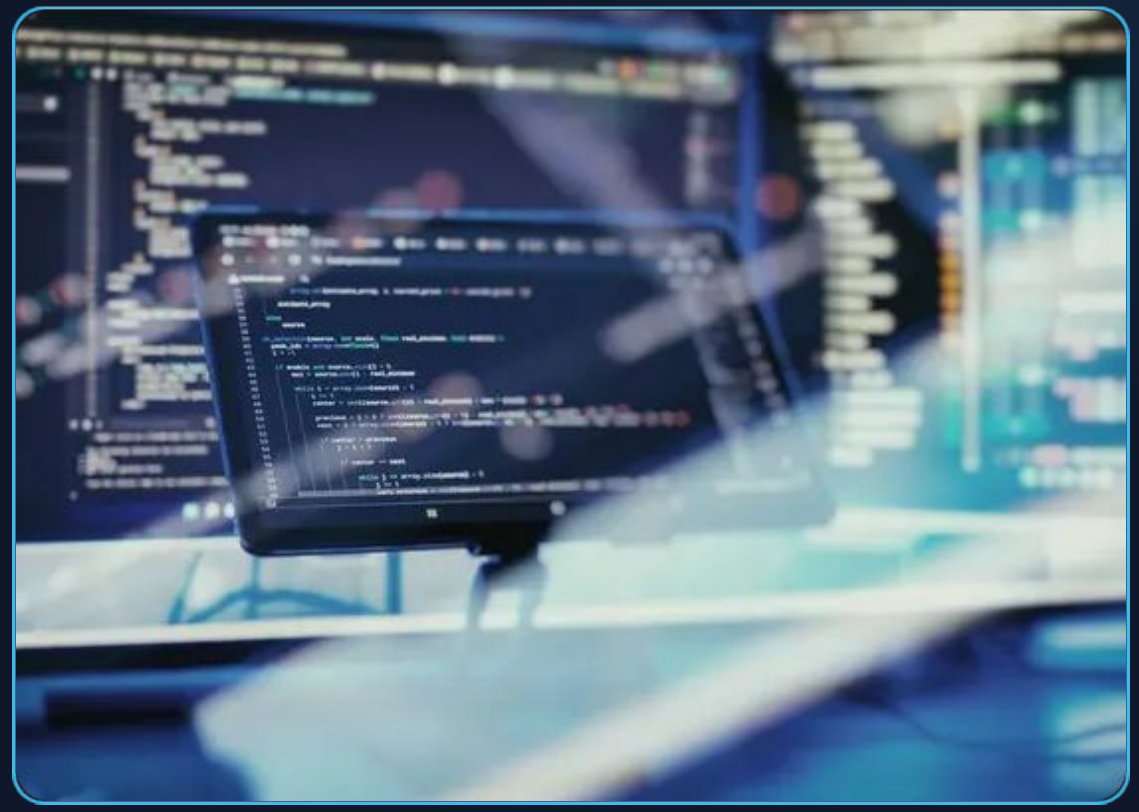
ESTUDIO PRÁCTICO: INYECCIÓN SQL (SQLI)

¿Cómo ocurre?

Falla en la sanitización de entradas, permitiendo que datos del usuario sean interpretados como comandos por la base de datos.

Tipos de SQLi

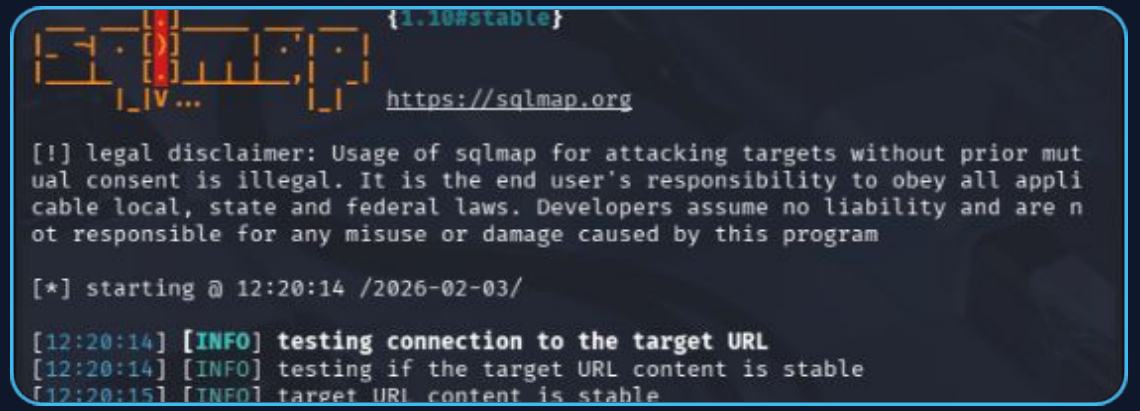
- Basada en errores.
- Consultas UNION.
- Inyección Ciega (Booleana/Tiempo).
- Consultas Apiladas (Stacked).



SIMULACIÓN AVANZADA CON SQLMAP

```
$ sqlmap -u "https://financiera.mx/login?id=1" --dbs
[INFO] testing 'PostgreSQL inline queries'
[INFO] fetching database names
available databases [3]:
[*] information_schema
[*] user_credentials_db
[*] public
```

Herramienta automática que elimina la necesidad de desarrollar código a medida, elevando la **Facilidad de Explotación a 9**.



MODELADO CUANTITATIVO: CASO SQLI

Probabilidad: ALTA

Skill: 5 | Motive: 4 | Opportunity: 9 |

Size: 9
Discovery: 9 | Exploit: 9 |

Awareness: 9 | Detect: 8

Score: 7.75

Impacto: ALTO

Conf: 9 | Integ: 7 | Avail: 5 | Acc: 9

Financ: 3 | Reput: 5 | Regul: 5 |

Privacy: 5

Score: 6.00

SEVERIDAD FINAL

CRÍTICO

Prioridad Absoluta de Remediación

GOBERNANZA: EL MODELO TAME

Criterios de la matriz de riesgos

Gravedad	×	Probabilidad	=	Impacto del riesgo
Insignificante		Muy probable		Bajo
Menor		Probable		Mediano
Moderada		Posible		Alto
Importante		No es probable		
Catastrófica		Muy improbable		

Transferir

Delegar a través de seguros o terceros.

Aceptar

Validar el riesgo bajo criterios de negocio.

Mitigar

Rediseñar lógica y aplicar controles.

Eliminar

Remover el servicio o código vulnerable.

EL COSTO DEL INCUMPLIMIENTO

Institución	Motivo de Sanción	Monto (MDP)
Intercam Banco	Deficiencias en controles internos	92 MDP
CI Banco	Fallas en medidas de seguridad	66 MDP
Vector Casa de Bolsa	Omisiones en reportes de riesgo	26 MDP

*Nota: El mayor riesgo no es la multa, sino la revocación de la licencia para operar.

HORIZONTE 2026: LA BOMBA DE TIEMPO

Infraestructura Obsoleta

La CNBV ha señalado que no tolerará sistemas legados que representen riesgos sistémicos para la nación.

- Auditorías de resiliencia obligatorias.
- Nuevas exigencias de RTO y RPO.
- Convergencia hacia IA para detección de anomalías.

SEGURIDAD EN EL CICLO DE VIDA (SDLC)

Fase	Tipo de Prueba	Beneficio
Codificación	Plugins de IDE	Retroalimentación inmediata.
Commit	SAST	Detección de debilidades lógicas.
Build	SCA	Seguridad en cadena de suministro.
Deploy	DAST	Fallas en tiempo de ejecución.

MITIGACIÓN MANDATORIA: CASO SQLI

Consultas Preparadas (Parameterized Queries)

La respuesta mandatoria ante el riesgo crítico de inyección SQL.

```
// Forma segura con parámetros tipados
$stmt = $pdo->prepare('SELECT * FROM users WHERE email = :email');
$stmt->execute(['email' => $userInput]);
```

Al separar la estructura del comando de los parámetros, el motor procesa el input como texto literal, bloqueando la ejecución no autorizada.

SUPERVISIÓN BASADA EN DATOS

El Futuro de la Regulación

La CNBV se encamina hacia una supervisión en tiempo real. La transparencia en la gestión de incidentes será el mayor diferenciador competitivo.

Registro de 10 Años

Obligación de mantener el histórico de todos los incidentes detectados por una década para auditorías retrospectivas.

SÍNTESIS PARA LA ALTA DIRECCIÓN

1. Gobernanza

La ciberseguridad es responsabilidad del Director General, no solo de TI.

2. Anticipación

Implementar SDF y configurar MTU antes de la fecha límite de 2026.

3. Metodología

Utilizar OWASP para priorizar inversiones basadas en riesgo real de negocio.

La Confianza es Frágil

"La inversión en ciberseguridad hoy no solo evita multas, sino que protege el activo más valioso: la confianza del cliente."

Preguntas y Respuestas

Sesión de diálogo con Ulises M. Álvarez

Ulises M. Álvarez

CISO del Poder Ejecutivo de Querétaro

Contacto institucional vía redes gubernamentales del Estado de Querétaro.

FIN DE LA PRESENTACIÓN

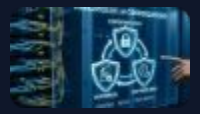
¡Gracias!

Por la resiliencia del sector financiero mexicano.

IMAGE SOURCES

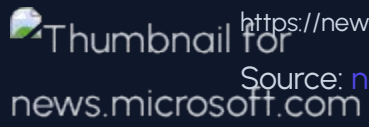
https://www.unir.net/wp-content/uploads/2023/01/ciso2.jpg

Source: www.unir.net



https://images.squarespace-cdn.com/content/v1/651dafa65543a16de7b078eb/fae5c0a7-6182-4259-af2c-4f13ecede17e/Gemini_Generated_Image_vqjswevqjswevqjs.png

Source: www.oxmtech.com



https://news.microsoft.com/wp-content/uploads/prod/sites/41/2021/04/square-cloud-1024x1024.jpg

Source: news.microsoft.com

https://www.prostay.com/_next/image/?url=%2Fimages%2Fblog%2Fhotel-security%2Fbanner.webp&w=2048&q=75

Source: www.prostay.com

https://www.practical-devsecops.com/wp-content/uploads/2026/02/owasp-risk-rating-methodology-vs-cvss.webp

Source: www.practical-devsecops.com

https://safetyculture.com/_next/image?url=https%3A%2F%2Fimages.ctfassets.net%2Fueprkma36dz5%2F5anJEQQpyQbmPf3rMlBPwx%2F047aca336a6a2a3001b0668488f39ff2%2FEjemplo-de-matriz-de-riesgo-5_C3_975.png&w=1920&q=65

Source: safetyculture.com

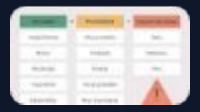
IMAGE SOURCES

https://st5.depositphotos.com/1052205/71053/i/450/depositphotos_710534374-stock-photo-work-home-programmer-coding-code.jpg

Source: depositphotos.com

https://cybermentor.net/wp-content/uploads/2026/02/sqlmap-running-en-sqli-labs.png

Source: cybermentor.net



https://assets.asana.biz/transform/e943f756-c33a-4e8c-b115-3bfe457bbf56/inline-project-planning-risk-matrix-template-2-es-2x

Source: asana.com

https://vilmanunez.com/wp-content/uploads/2026/02/el-futuro-de-la-inteligencia-artificial-segun-el-Foro-Economico-Mundial-Davos-2026.-Blog-de-Vilma-Nunez-portada.png

Source: vilmanunez.com

https://thumbs.dreamstime.com/b/profesional-de-negocios-pie-frente-una-gran-audiencia-en-un-moderno-sal%C3%B3n-conferencias-bajo-luces-azules-y-moradas-simbolizando-418525973.jpg

Source: es.dreamstime.com