QMA — QUALITY MANAGEMENT ASSOCIATES

CHECKLIST · READINESS

Checklist Art-18/36 Ley de Ciberseguridad MX

12 acciones para que un CISO mexicano llegue listo a la entrada en vigor de la Ley de Ciberseguridad. Basado en la iniciativa Colosio-MORENA (Senado, 30-abril-2025).

PARA
CISOs · Direcciones de TI · Compliance · Operadores regulados.

CUÁNDO
Iniciativa presentada en el Senado en abril 2025. Publicación DOF esperada S2-2026.

CÓMO SE USA
12 acciones secuenciales. Cada una ancla un artículo concreto de la Ley.

BLOQUE 1 — CIMIENTOS: GOBERNANZA, CRITICIDAD Y PLAN IR

De jure: instalar la figura del CISO y el plan de respuesta

La Ley designa dos figuras formales — el **enlace especializado en ciberseguridad** (art 18, aplicable a las cinco categorías de sujetos obligados) y la **persona responsable de ciberseguridad** (art 36 fr III, específica de operadores). Funcionalmente convergen en el rol del CISO. Estas primeras seis acciones instalan la gobernanza obligatoria antes de que la Agencia la pida.

01 **Designación formal del CISO** ART 18 · ART 36 FR III

Acta del Consejo o policy interna designando un *enlace especializado en ciberseguridad*. Documente: nombre, línea de reporte directa al Consejo, alcance de responsabilidad sobre los activos críticos, dedicación esperada. Es la primera evidencia que la Agencia pedirá en una auditoría.

02 **Auto-clasificación de criticidad de la organización** ART 30

Determine si su organización cae en **Alta** (ICI + OSE estratégicos), **Media** (OSE no estratégicos + grandes SDR) o **Baja** criticidad. La clasificación se revisa cada dos años (art 31) — anticípese a saltar de Baja a Media si su huella de datos crece.

03 **Evaluación de riesgos documentada** ART 37

Anual para Alta y Media criticidad; autoevaluación anual para Baja. Use el lenguaje del art 3 de la Ley: identifique *amenazas cibernéticas*, *activos críticos de información*, *vulnerabilidades* y el *riesgo cibernético* resultante con probabilidad × impacto.

04 **Auditoría externa de ciberseguridad bienal** ART 37

Auditor externo acreditado, mínimo cada dos años para Alta y Media criticidad. Hágalo conforme a estándares internacionales (ISO 27001:2022, NIST CSF 2.0, equivalentes sectoriales). Los resultados se remiten a la Agencia. Empiece la búsqueda de auditor doce meses antes de la fecha objetivo.

05 **Plan de respuesta a incidentes con flujos documentados** ART 36 FR I

Procedimientos escritos para detección, contención, erradicación, recuperación y lecciones aprendidas. Incluya umbrales de severidad, roles, líneas de comunicación con la Agencia y con personas afectadas. Pruebe con un tabletop al menos una vez al año.

06 **Canal seguro de comunicación con la Agencia** ART 36 FR II

Cifrado, no público, documentado en el plan IR. Defina hoy el método (correo cifrado dedicado, plataforma sectorial, canal MP) y mantenga el contacto operativo actualizado.

Plazo concreto de reporte (mito de las 72 horas): la Ley no fija plazo en horas. El art 26 obliga a notificar "oportuna y proporcionadamente" y delega el plazo concreto a los protocolos secundarios que emitirá la propia Agencia (Transitorio Octavo, 12 meses post-vigencia). El único plazo en horas

dentro del articulado es el del art 41 — 24 horas — pero corre de la Agencia hacia las autoridades de gobierno, no de las empresas hacia la Agencia. Cualquier consultor que le venda preparación para "el plazo de 72 horas de la Ley" está extrapolando.

BLOQUE 2 — OPERACIÓN CONTINUA Y DERECHOS DIGITALES

De facto: capacidad operativa que la Agencia querrá ver

Las seis acciones siguientes pasan del papel a la operación. Son las capacidades que una auditoría técnica de la Agencia (art 22) verificará en campo: capacitación efectiva, post-mortems con causa raíz, continuidad probada, divulgación responsable de vulnerabilidades y derechos digitales de las personas afectadas por sus servicios.

07 **Capacitación continua del personal con métricas** ART 33 FR II.A · ART 38

Programa anual con cobertura, frecuencia, evaluación efectiva y resultados. La Ley exige cultura de ciberseguridad — buenas prácticas, ética digital y gestión de riesgos en todos los niveles. Documente quién recibió qué entrenamiento y cuándo.

08 **Procedimiento de análisis post-incidente con causa raíz** ART 36 FR IV

Plantilla escrita: descripción, timeline, causa raíz, daño económico/operativo, acciones de remediación, mejora preventiva. Conserve los post-mortems — son la evidencia que la Agencia pedirá si vuelve a ocurrir un incidente similar.

09 **Plan de continuidad operativa con simulacro anual** ART 23 · ART 30 FR I

Para servicios esenciales: defina RTO, RPO, sitios alternos, dependencias de proveedores, comunicación a clientes. Ejercite el plan con un simulacro de incidente al año. Conserve el reporte del simulacro como evidencia de resiliencia.

10 **Interoperabilidad segura con CERT sectorial / Nacional** ART 39 · ART 43

Si su sector es de Alta o Media criticidad, el CERT sectorial será obligatorio. Identifique hoy quién lo liderará en su sector, establezca un mecanismo de intercambio técnico (formato, cifrado, frecuencia) y participe en ejercicios conjuntos cuando se anuncien.

11 **Política de divulgación responsable de vulnerabilidades** ART 25 FR VIII · ART 29

Canal para que terceros (researchers, clientes, empleados) reporten vulnerabilidades en sus sistemas con confidencialidad. La Agencia exige proteger la identidad del notificante. security.txt en su sitio + correo dedicado + SLA de respuesta.

12 **Procedimiento de notificación a personas afectadas** ART 7 FR V · ART 25 FR IX

Cuando un incidente comprometa datos personales o servicios esenciales, las personas afectadas tienen derecho a ser informadas oportuna y verazmente, y a acceder a mecanismos de reparación, bonificación o compensación. Plantillas pre-aprobadas + criterios de activación documentados.

Sanción más severa operativamente: el régimen sancionatorio del Título X (arts 59-64) contempla cuatro sanciones graduables: amonestación, multa proporcional, suspensión temporal de operaciones e **inhabilitación para prestar servicios esenciales** por reincidencia grave. La Ley no fija montos en pesos — pasan a reglamentación secundaria. La inhabilitación es la sanción que opera como expulsión del mercado regulado. Las primeras seis acciones de este checklist son el blindaje contra ella.

CIERRE — CALENDARIO OPERATIVO Y SIGUIENTE PASO

Doce meses: la ventana real de preparación

Asumiendo publicación DOF en el segundo semestre de 2026 y designación del Director General de la Agencia en los primeros 180 días posteriores (Transitorios 2° y 3°), las obligaciones operativas mordieron a su organización entre el segundo semestre de 2027 y el primer trimestre de 2028. Esa es la ventana real de preparación.

01 **Mes 0 a 3 — Diagnóstico estructural**
Acciones 1-2 de este checklist: designación CISO y auto-clasificación de criticidad. Mapeo de activos críticos y candidatos a inclusión en el RICI.

02 **Mes 3 a 6 — Plan IR y políticas internas**
Acciones 5-7: plan de respuesta a incidentes documentado, canal seguro con la Agencia, política interna anclada al art 33 con calendario de capacitación.

03 **Mes 6 a 9 — Auditoría externa y certificación**
Acciones 3-4: evaluación de riesgos + auditoría externa. ISO 27001 / NIST CSF 2.0 / equivalente sectorial.

04 **Mes 9 a 12 — Resiliencia y simulacros**
Acciones 8-12: simulacro de continuidad, interoperabilidad CERT, política de divulgación, plantillas de notificación a afectados.

Continúe con la cobertura editorial

El Hub **Ley de Ciberseguridad en México** de QMA mantiene un análisis vivo de los 64 artículos, 10 títulos y 9 transitorios. Se actualiza con cada cambio del proceso legislativo en el Senado.

→ qma.mx/ley-ciberseguridad-mexico

Suscríbase al **Observatorio Legislativo de Ciberseguridad** para recibir una actualización cada dos semanas con el avance del proceso y guías operativas para CISOs mexicanos.

Fuente primaria. Iniciativa con proyecto de decreto por el que se expide la Ley de Ciberseguridad, presentada en el Salón de Sesiones del Senado de la República el 30 de abril de 2025 por el senador Luis Donaldo Colosio Riojas (MC) y la senadora Lucía Trasviña Waldenrath (MORENA). Gaceta del Senado, LXVI Legislatura.

Marcos complementarios. Política General de Ciberseguridad para la Administración Pública Federal (DOF 18-dic-2025), Plan Nacional de Ciberseguridad 2025-2030, Código Penal Federal arts 211 bis 1-7, Convenio de Budapest (2001), Convención ONU contra la Ciberdelincuencia (diciembre 2024).

Sobre QMA. QMA es una consultora de ciberseguridad gestionada (MSSP) con cobertura editorial dedicada a marcos regulatorios y prácticas CISO en México y Latinoamérica.