

Estudio · Ciberseguridad gubernamental en México

Radar Estatal de Ciberseguridad México 2026

Las 32 entidades bajo el mismo criterio

Qué leyes, reglamentos e instrumentos del Ejecutivo imponen deberes de ciberseguridad a los gobiernos estatales, dónde falta el instrumento que la ley ordena y cómo se compara Sonora con los estados más avanzados.

CORTE 22-oct-2026 cotejo con fuente oficial	ALCANCE 32 entidades leyes, reglamentos y acuerdos	AUTORA Marcela Mexía Transformation Trends	EDICIÓN Octubre 2026 versión pública
---	--	--	--

Corte de información: 22 de octubre de 2026. Las citas que sostienen la clasificación de cada entidad, las cifras del resumen y la sección de datos personales se cotejaron con la publicación oficial disponible; las excepciones se indican en el texto y en la tabla de las 32 entidades. **Declaración de interés:** Transformation Trends ofrece capacitación y certificaciones en ciberseguridad, seguridad de la información e inteligencia artificial, y participa con propuestas en el parlamento abierto sobre la iniciativa de Ley de Transformación Digital de Sonora que este estudio analiza.

01

Resumen ejecutivo

Al 22 de octubre de 2026, **en las fuentes revisadas no identificamos ninguna ley estatal cuyo título u objeto principal sea la ciberseguridad.** Lo que de verdad distingue a las entidades es otra cosa: si sus leyes imponen deberes de seguridad a las dependencias y si el instrumento que esas leyes ordenan existe.

- **8 de 32 entidades** tienen en ley, reglamento o ley orgánica al menos un deber fuerte de ciberseguridad, y **otras 4** lo prevén de forma permisiva, parcial o condicionada (casos límite). **8** solo tienen deberes genéricos, **2** dependen de instrumentos del Ejecutivo sin rango de ley y **10** no tienen instrumento estatal específico identificado.
- **Las 32 están sujetas al piso nacional:** la Ley Nacional para Eliminar Trámites Burocráticos (LNETB), la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y la Ley General de Archivos. La Política General de Ciberseguridad (DOF 17-dic-2025) solo obliga a la Administración Pública Federal (APF).
- **En 5 de los 8 casos fuertes plenos no localizamos publicado el programa, estándar o norma que la ley ordena.** En 3 de ellos (Chiapas, Chihuahua y Tamaulipas), el deber que los clasifica depende de ese instrumento; Guerrero y Sonora se clasifican por deberes que operan sin él.
- **Ninguna ley estatal revisada, ni el Reglamento de Sonora, el único revisado de forma sistemática, fija un plazo en horas para notificar incidentes de ciberseguridad a una autoridad ni nombra ISO/IEC 27001 o NIST.** Morelos es la única entidad identificada cuya ley obliga a sus dependencias a notificar incidentes, "de inmediato" y a la Agencia estatal. Los controles más concretos identificados (autenticación multifactor, EDR, reporte inmediato, auditorías) están sobre todo en acuerdos del Ejecutivo de Michoacán, Querétaro y la Ciudad de México.
- **El plazo de 72 horas para avisar vulneraciones de datos personales se conserva en al menos cinco leyes estatales no armonizadas.** La LGPDPPSO de 2025 ordena avisar "sin dilación alguna", sin fijar horas.
- **La operación puede ir por delante de la ley.** El único CSIRT de un gobierno estatal registrado en FIRST, el ADEM-CERT del Estado de México, pertenece a una entidad que en el plano normativo es apenas caso límite.

-
- **En la agenda legislativa** hay iniciativas de Ley de Ciberseguridad en Nuevo León (dos) y en la Ciudad de México (una), sin dictamen localizado. En el plano federal, la iniciativa de ley general de una senadora daría a los estados 180 días para crear una coordinación estatal de ciberseguridad.
-
- **Sonora** figura entre los casos fuertes por su ley y su reglamento: la Ley de Gobierno Digital obliga a los Entes a cumplir lineamientos sobre incidentes de seguridad, que no localizamos publicados, y el Reglamento de 2024 les ordena informar a la Subsecretaría de Gobierno Digital tras cada vulneración. La iniciativa de Ley de Transformación Digital (Folio 04605, recibida el 5 de octubre de 2026) propone avisar los incidentes de ciberseguridad en máximo doce horas: aprobada así, sería la primera ley estatal identificada con un plazo en horas para ese aviso. No define qué es un incidente, no prevé auditorías periódicas y no designa un equipo de respuesta a incidentes.

El radar describe el marco normativo. No mide madurez, cumplimiento ni operación de los gobiernos estatales.

02

Método y criterio

Cada entidad recibe la categoría del instrumento **vigente** de mayor rango que identificamos al 22 de octubre de 2026. Buscamos, para las 32 entidades: ley específica de ciberseguridad e iniciativas de esa ley; ley de gobierno digital, electrónico u orgánica equivalente y, cuando se localizó, su reglamento; instrumentos del Ejecutivo con obligaciones de seguridad; armonización con la reforma constitucional del 15 de abril de 2025 y con la LNETB; y, sin pretensión de exhaustividad, reformas penales.

Privilegiamos los periódicos oficiales, los portales de los congresos y las compilaciones de la Suprema Corte y de la Cámara de Diputados. Cuando solo hubo una copia no oficial (Justia, mley.mx) o una nota de prensa, lo indicamos y bajamos la confianza. Las citas se extrajeron de forma automatizada y el 22 de octubre de 2026 cotejamos contra la publicación oficial las que sostienen la clasificación de cada entidad, las cifras del resumen y la sección de datos personales; donde no hubo publicación oficial accesible, lo indicamos. Los textos escaneados se leyeron con reconocimiento óptico de caracteres. Las iniciativas legislativas se reportan con la fuente indicada y no se cotejaron una por una.

Los cinco niveles

-
- **Fuerte.** La ley, su reglamento o la ley orgánica contiene, con fórmula imperativa ("deberá") o declaratoria de obligatoriedad ("de observancia obligatoria"), al menos uno de estos elementos: (a) un programa, plan, sistema o política de ciberseguridad nombrado y obligatorio para los sujetos; (b) un deber de notificar o informar incidentes a una autoridad estatal; (c) auditorías, evaluaciones de seguridad o simulacros de alcance general; (d) deberes de protección de activos críticos; (e) una facultad expresa para emitir normas de seguridad de la información o ciberseguridad que el texto declare obligatorias para los sujetos.
-
- **Fuerte, caso límite.** El elemento se cumple solo con verbo permisivo ("podrán"), con alcance parcial o con aplicación condicionada a una declaratoria o un reglamento pendiente.

- **Genérico.** Ley de gobierno digital, electrónico u orgánica con deberes o atribuciones de seguridad que no alcanzan el umbral.
- **Instrumento del Ejecutivo.** No hay ley de ese tipo, pero sí una política o guía administrativa con obligaciones de seguridad.
- **Sin instrumento estatal específico identificado.** Solo leyes de firma electrónica, mejora regulatoria o datos personales. Aplica el piso nacional.

No cuentan como deber fuerte: los principios sin deber (incluidas las copias del art. 6 fr. XIII y del art. 25 de la LNETB), los "controles efectivos", la fórmula de seguridad del expediente de trámites, la firma electrónica, los datos personales ni las atribuciones de una autoridad que no generan deberes para los sujetos. Las **iniciativas** se reportan aparte porque no tienen efectos jurídicos. Lo **penal** no se investigó en las 32 entidades y no forma parte de la escala.

Cuánto pudimos leer

La afirmación de que no hay leyes estatales de ciberseguridad descansa en el listado oficial de leyes que publica cada congreso. Ese listado no se pudo leer igual en todas las entidades.

Lectura del listado oficial	Entidades	N.º
Completa	Campeche, Chiapas, Chihuahua, Coahuila, Guerrero, Hidalgo, Nayarit, Puebla, San Luis Potosí, Sinaloa, Tabasco, Tamaulipas, Yucatán y Zacatecas	14
Búsqueda manual por palabras clave en el portal oficial (22-oct-2026)	Aguascalientes, Baja California, Baja California Sur, Ciudad de México, Colima, Durango, Estado de México, Guanajuato, Jalisco, Michoacán, Morelos, Nuevo León, Oaxaca, Quintana Roo, Tlaxcala y Veracruz	16
No se pudo leer	Querétaro y Sonora	2

En las 16 entidades sin lectura automática completa, el 22 de octubre de 2026 buscamos a mano en el portal oficial con los términos ciberseguridad, seguridad de la información, seguridad informática, gobierno digital y gobierno electrónico. En Querétaro, cuyo portal no respondió, y en Sonora, la ausencia descansa en la compilación de Justia (última actualización indicada: 26 de mayo de 2026) y en búsquedas en los dominios de los congresos. **"No identificado" significa que no lo encontramos en las fuentes consultadas, nunca que no exista**, y no identificar un instrumento no equivale a incumplimiento.

Otro límite: solo revisamos de forma sistemática el reglamento de Sonora. La confianza es alta si se leyó el texto oficial completo, media si la lectura fue parcial, en copia no oficial o con un condicionante abierto, y baja si el dato no se pudo contrastar.

Declaración de interés

Transformation Trends S.A. de C.V. vende capacitación y certificaciones en ciberseguridad, seguridad de la información, inteligencia artificial y sistemas de gestión: certificaciones ISO, entre ellas ISO/IEC 27001, como PECB Authorized Partner, y certificaciones de EC-Council como EC-Council Accredited Training Center (ATC). Transformation Trends financió este estudio con recursos propios; no recibió fondos de ningún gobierno ni de otras empresas. Algunos vacíos que el estudio señala, como las auditorías periódicas, los estándares y la capacitación, corresponden a servicios que Transformation Trends ofrece. Transformation Trends participa

con propuestas en el parlamento abierto sobre la iniciativa de Ley de Transformación Digital de Sonora, que este estudio analiza (mesa de Ciudad Obregón, 23 de octubre de 2026).

Para limitar el sesgo, el estudio no infiere demanda de certificación a partir de los instrumentos, no recomienda productos, proveedores ni certificaciones y menciona normas técnicas solo cuando el propio instrumento las cita. Ningún instrumento estatal vigente identificado exige certificarse en ISO/IEC 27001 ni adoptar NIST como obligatorio.

03

Ninguna ley estatal tiene la ciberseguridad como objeto principal

La única ley con "cibernético" en el título que localizamos es de prevención del delito, no de gestión. La [Ley de Prevención de Delitos Cibernéticos para el Estado de Sonora](#) (Ley 85, B.O. 23-dic-2019) establece las bases para programas de prevención mediante consejos estatal y regionales. No usa "ciberseguridad" ni impone a las dependencias deberes de seguridad de sus sistemas ni de notificación de incidentes: su art. 28 solo les pide prever presupuesto para esos programas ([dictamen](#)). La leímos en Justia; el documento del Congreso consigna su publicación (B.O. núm. 51, sección IV, 23-dic-2019) sin reformas registradas, pero no confirmamos su vigencia en una compilación oficial.

Lo más cercano a una ley de ciberseguridad son **capítulos con nombre propio dentro de leyes de gobierno digital**: el Capítulo IX "De la Ciberseguridad" (arts. 87 y 88) de la [Ley de Gobernanza Digital de Tlaxcala](#); la sección del Programa Anual de Ciberseguridad Gubernamental de la [Ley de Gobierno Digital de Chiapas](#), que además pone la ciberseguridad gubernamental entre sus objetos (art. 1 fr. V); el capítulo De la Ciberseguridad del Centro de Datos (arts. 115 a 118) de la Ley de Transformación Digital de Morelos; y el capítulo "Seguridad de la información" (arts. 55 a 57) de la [Ley de Ciudadanía Digital de la Ciudad de México](#). Ninguna de esas leyes tiene la ciberseguridad como objeto principal; el criterio las evalúa como leyes de gobierno digital.

Cuatro iniciativas, ninguna dictaminada

Las iniciativas no clasifican en el radar porque no tienen efectos jurídicos. No leímos el articulado de ninguna de las tres estatales: su contenido proviene de comunicados y prensa.

Ámbito	Iniciativa	Presentación	Estatus al corte	Contenido conocido
Nuevo León	Ley de Ciberseguridad de una diputada de Movimiento Ciudadano	Turnada el 15-ene-2025 a la Comisión de Justicia y Seguridad Pública (cartera)	Sin dictamen localizado; en la agenda mínima del Congreso (Acuerdo 175)	Oficina estatal de ciberseguridad, política general anual y unidades en dependencias estatales y municipales (comunicado)
Nuevo León	Ley de Ciberseguridad de los grupos de MORENA, PT y PVEM	Turnada el 8-sep-2025 a la misma comisión (cartera)	Sin dictamen localizado	Sistema Estatal de Ciberseguridad para coordinar, prevenir y responder a incidentes (comunicado)

Ámbito	Iniciativa	Presentación	Estatus al corte	Contenido conocido
Ciudad de México	Ley de Ciberseguridad del INFO CDMX	13-may-2025 (Crónica)	Sin dictamen localizado; la nueva Ley de Transparencia (13-jul-2026) ordena extinguir al promovente (guía del INFO CDMX)	Notificar al Instituto los incidentes que pudieran vulnerar datos personales, sin plazo conocido (prensa)
Federal	Ley General para la Coordinación de la Ciberseguridad, de la senadora Jesús Lucía Trasviña Waldenrath (Morena)	Gaceta Parlamentaria del 7-ene-2026 (texto)	Turno y estatus no verificados	Registro Estatal de Incidentes Cibernéticos (art. 22 fr. V) y 180 días para que los estados creen una Coordinación Estatal de Ciberseguridad (transitorio Quinto)

Fuera de estos casos solo hay rastros sin verificar: una iniciativa ciudadana de San Luis Potosí de 2020, sin movimiento visible desde agosto de 2021, y documentos de Guanajuato y Michoacán que aparecieron en búsquedas y no pudimos abrir. La afirmación de un senador de que una ley federal "ya fue aprobada en comisiones" no tiene dictamen identificado ([El Financiero](#)).

04

El piso nacional obliga a las 32 entidades; solo la APF tiene plazo de reporte

Ninguna entidad carece de obligaciones de seguridad de la información: tres leyes generales o nacionales ya las imponen a todos los gobiernos estatales y municipales. Entre los instrumentos revisados que obligan a gobiernos, el único con plazo en horas para reportar incidentes es federal y solo alcanza a la APF.

Instrumento	Rango y fecha	¿Obliga a estados y municipios?	Contenido de seguridad
LNETB	Ley nacional, DOF 16-jul-2025	Sí (art. 3 fr. XXXIV)	Principio de ciberseguridad (art. 6 fr. XIII); criterios de seguridad para el área estatal de soluciones tecnológicas (art. 25 frs. IV a VI); responsabilidad administrativa genérica (art. 113). Sin notificación de incidentes ni CSIRT
LGPDPPO	Ley general, DOF 20-mar-2025	Sí	Medidas de seguridad (art. 25), documento de seguridad (art. 29), bitácora (art. 33) y aviso de vulneraciones "sin dilación alguna" (art. 34)
Ley General de Archivos	Ley general, DOF 15-jun-2018	Sí	Programa de seguridad de la información que garantice la continuidad de la operación (art. 60 fr. I) y controles en estructura organizacional, clasificación de activos, recursos humanos, seguridad física, control de acceso, desarrollo de sistemas y continuidad (fr. II)
Política General de Ciberseguridad	Acuerdo de la ATDT federal, DOF 17-dic-2025	No: solo la APF	Titular institucional en 60 días; incidentes críticos en 24 horas o menos como función del CSIRT Nacional-APF; curso obligatorio por establecer

Instrumento	Rango y fecha	¿Obliga a estados y municipios?	Contenido de seguridad
LFPDPPP	Ley federal, DOF 20-mar-2025	No a los gobiernos; sí a las empresas	Medidas de seguridad (art. 18) y aviso inmediato de vulneraciones al titular (art. 19)
LGSNSP	Ley general, DOF 16-jul-2025	Sí, en seguridad pública	Sin deberes de ciberseguridad
Pacto Nacional para la Implementación de la LNETB	Acuerdo político-administrativo firmado el 18-ago-2026; aviso en el DOF del 28-sep-2026	Firmado por las 32 entidades	Ningún compromiso de ciberseguridad entre los que enumera el DOF (Aviso)

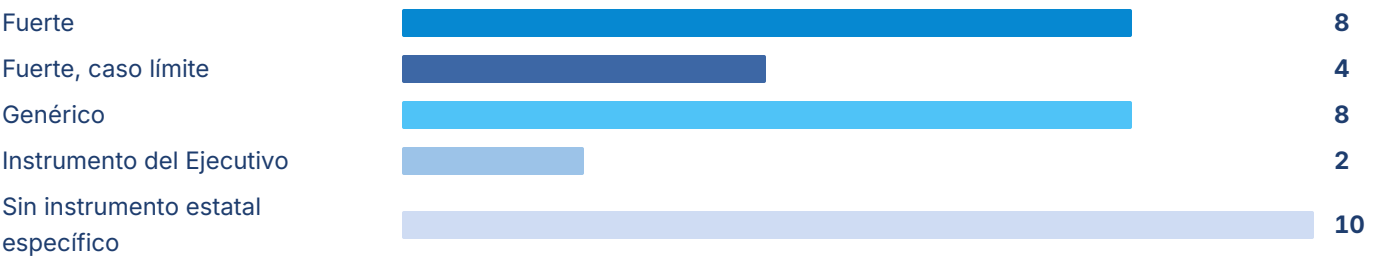
La LNETB es piso de principio y de diseño, no un régimen de gestión. Pide que en las soluciones tecnológicas "se adopten los protocolos de seguridad de la información y comunicaciones necesarias" (art. 6 fr. XIII). Su art. 25 obliga a cada entidad federativa a tener un área de desarrollo de soluciones para digitalizar trámites, que "deberá observar" criterios de seguridad y estándares "para prevenir y reaccionar ante amenazas o ataques cibernéticos"; los municipios sin capacidad pueden suplirla por convenio. No nombra estándares ni exige reportar incidentes. Su transitorio Décimo Tercero dio a los congresos locales 180 días naturales para armonizar, plazo que concluyó el 12 o el 13 de enero de 2026 según se cuente el día inicial (cálculo propio; transitorio cotejado en el DOF vespertino del 16 de julio de 2025).

El plazo de 24 horas no está en el Acuerdo sino en el documento de la Política, entre las funciones del CSIRT Nacional-APF ("incidentes críticos deberán reportarse en ≤ 24 h"), sin definir qué es un incidente crítico. El curso obligatorio para servidores públicos es una acción por establecer, y NIST, ISO y CIS Controls figuran solo como referencias ([Política, p. 41 y AO7 en p. 34](#)). Para los estados es, cuando mucho, un modelo.

La armonización local con la LNETB casi nunca incorpora ciberseguridad. Las dos reformas constitucionales locales publicadas, la del Estado de México (Decreto 261, 22-ene-2026) y la de Sinaloa (Decreto 397, 25-may-2026), la omiten. Tamaulipas es el único caso en que la misma ley orgánica concentra la autoridad de simplificación y la facultad de emitir normas obligatorias de seguridad de la información ([P.O. Tamaulipas](#)).

Para las empresas, el deber de seguridad viene de la LFPDPPP, no de las leyes estatales. Toda empresa que trate datos personales debe mantener medidas de seguridad y avisar de inmediato las vulneraciones al titular, con multas de hasta 320,000 UMA (art. 59). Ninguna ley estatal revisada añade a las empresas deberes de gestión de ciberseguridad; donde aparecen particulares es como proveedores del gobierno, por contrato o por reglamento (Sonora).

Ocho entidades con deberes fuertes y cuatro casos límite; en tres, el deber depende de un instrumento no localizado



Clasificación de Transformation Trends con el criterio de la sección de método · 32 entidades · corte y cotejo al 22-oct-2026

En cinco de los ocho casos fuertes plenos no localizamos publicado el programa, estándar o norma que la ley ordena. En tres (Chiapas, Chihuahua y Tamaulipas), el deber que los clasifica depende de ese instrumento. Guerrero y Sonora se clasifican por deberes que operan sin él: las auditorías al menos bienales de la ley de Guerrero (art. 55) y, en Sonora, el informe a la Subsecretaría tras cada vulneración que exige su Reglamento (art. 130). Mandato y controles no coinciden: hay casos fuertes cuyo programa no aparece publicado y casos genéricos, como Michoacán, con controles concretos por la vía del Ejecutivo.

Qué dispara cada caso fuerte

Entidad	Instrumento y disparador	Notificación de incidentes	Auditoría o simulacro	Instrumento ordenado
Chiapas	Ley de Gobierno Digital: Programa Anual de Ciberseguridad Gubernamental "aplicable a todos los Sujetos Obligados" (art. 9 fr. XVI), presentado a más tardar en junio (art. 25)	No	No	No localizado
Chihuahua	Ley de Gobierno Digital: Programa de Seguridad Informática que "deberán ser observados por las dependencias y entidades" (arts. 22 fr. IX y 32)	No	No	No localizado
Ciudad de México	Ley de Operación e Innovación Digital: lineamientos de seguridad informática para los Entes (art. 32 fr. XIII); Ley de Ciudadanía Digital: auditoría al menos cada dos años (art. 57)	"De manera inmediata", en lineamientos del Ejecutivo	Sí, al menos bienal	Lineamientos de 2020
Guerrero	Ley 679 de Gobernanza Digital: auditorías de ciberseguridad al menos cada dos años (art. 55); desacato a los lineamientos, que la ley califica como "Falta Grave" (art. 61, en reforma)	No	Sí, al menos bienal	Estrategia estatal no localizada

Entidad	Instrumento y disparador	Notificación de incidentes	Auditoría o simulacro	Instrumento ordenado
Morelos	Ley de Transformación Digital: las dependencias "estarán obligadas a notificar de inmediato a la Agencia cualquier incidente o vulnerabilidad", bajo responsabilidad administrativa (art. 116); Centro de Operaciones de Seguridad a cargo de la Agencia (art. 118)	Sí, "de inmediato", por ley (art. 116)	Evaluación periódica a cargo de la Agencia (art. 118 fr. VI)	No lo requiere: deber directo
Querétaro	Ley de Gobierno Digital: estándares mínimos de seguridad de la información "que deben de cumplir los sujetos" (art. 12 fr. IX); decisiones obligatorias de la Comisión (art. 11)	"De manera inmediata", en disposiciones del Ejecutivo	Plan de recuperación probado al año (disposiciones)	Disposiciones TIC de 2025
Sonora	Ley 173 de Gobierno Digital: lineamientos de incidentes de seguridad que emite la Oficialía Mayor (art. 71 fr. XVI) y que los Entes deben cumplir (art. 74 fr. IX). Reglamento: los Entes "deberán establecer" medidas de seguridad (art. 127); informe de acciones correctivas tras una vulneración (art. 130)	Informe posterior con plazo supletorio de 10 días hábiles (art. 3); aviso inmediato de proveedores por contrato (art. 83)	No	Lineamientos de incidentes no localizados; Reglamento publicado
Tamaulipas	Ley Orgánica de la Administración Pública: normas de seguridad de la información, ciberseguridad y atención de incidentes "de observancia obligatoria" (art. 42 Bis frs. IV y V)	Materia de las normas por emitir	No	Normas no localizadas
Nayarit (caso límite)	Ley de Gobierno Digital: los sujetos deben cumplir los Estándares (art. 23 fr. IV), pero el rubro de seguridad es opcional ("podrán", art. 18 fr. VIII); solo son obligatorios los protocolos de seguridad para registros con datos personales (art. 53)	No	No	Estándares no localizados
Estado de México (caso límite)	Ley de Gobierno Digital: Estándares con "Administración de la seguridad" (art. 19 fr. IX) que los sujetos "deberán observar" (art. 21), anclados a los portales	No	No	Publicación no verificada
Tabasco (caso límite)	Ley de Gobierno Digital y Firma Electrónica: materia de seguridad de los Estándares con verbo permisivo (art. 18 fr. VIII); auditorías solo para la Ventanilla Digital (art. 47 Novodecies)	No	Solo la Ventanilla	No verificado
Tlaxcala (caso límite)	Ley de Gobernanza Digital: medidas de ciberseguridad para activos críticos (art. 67 fr. V); aplicación sujeta a una declaratoria del Ejecutivo (transitorio Primero)	No	Simulacros a cargo de la Agencia (art. 88 fr. I)	Declaratoria no localizada

Las fuentes de cada fila están en la tabla de las 32 entidades. Morelos pasó de genérico a fuerte en el cotejo: su deber de notificar está en el art. 116, que no habíamos podido leer en la primera revisión. Nayarit pasó de

fuerte a caso límite: su rubro de estándares de seguridad es opcional ("podrán", art. 18 fr. VIII), como el de Tabasco, y el único deber obligatorio (art. 53) protege registros con datos personales. En Chihuahua, el primer Programa de Seguridad Informática debe emitirse dentro del año siguiente a la publicación del primer Programa Especial (transitorio Noveno), y el Consejo que debe aprobarlo se instaló hasta el 15 de julio de 2026. Sonora tampoco tiene localizados los lineamientos de incidentes que ordena su ley; su clasificación se sostiene además en el Reglamento, que obliga a entregar a la Subsecretaría un informe tras cada vulneración (art. 130, vía b). El deber de establecer las medidas "que resulten necesarias" (art. 127) no alcanzaría el umbral por sí solo. Dos sensibilidades del criterio: si la vía (a) exigiera que el verbo se dirija a los sujetos, Chiapas pasaría a caso límite; y en Guerrero, el Congreso aprobó el 22 de septiembre de 2026 una reforma a los arts. 61 y 62, de sanciones, cuyo texto no verificamos ([Digital Guerrero](#)).

Las leyes de gobierno digital comparten una plantilla

Las leyes de Querétaro y el Estado de México incluyen la "Administración de la seguridad" en su catálogo obligatorio de estándares, y la de Nayarit la prevé como rubro opcional ("podrán", art. 18 fr. VIII). En el grupo genérico, las de Puebla, Durango, Sinaloa y Michoacán no tienen ese rubro en el texto revisado; la de Aguascalientes, de medios digitales, pide respaldo, recuperación y seguridad (art. 14); Coahuila y Nuevo León tienen leyes de gobierno electrónico centradas en firma y conservación, y Jalisco entra solo por su Ley Orgánica, que faculta a aprobar estándares de seguridad sin declararlos obligatorios (art. 19 fr. XXXIII). Es el caso más débil del grupo: su ley se ocupa de la seguridad, pero no impone deberes a las dependencias.

Los controles más concretos están en el Ejecutivo

- **Michoacán**, [Políticas Generales en Materia de Ciberseguridad](#) (P.O. 17-oct-2024): autenticación multifactor, contraseñas de al menos 12 caracteres, capacitación obligatoria (anual como recomendación, "lo ideal será"), auditorías y reporte de incidentes de contraseñas "a la brevedad posible".
- **Querétaro**, [Disposiciones TIC](#) (11-jul-2025): reporte "de manera inmediata" al Equipo de Seguridad, doble factor, EDR y plan de recuperación probado al menos una vez al año, solo para el Ejecutivo.
- **Ciudad de México**, [Lineamientos de Seguridad de la Información](#) (GOCDMX 26-mar-2020): sistema de gestión de seguridad de la información con auditorías internas, responsable por Ente, capacitación y reporte "de manera inmediata", con alcance sobre las alcaldías. Es el instrumento ejecutivo más completo de los revisados.
- **Quintana Roo**, [Guía de Ciberseguridad](#) de la Agencia de Transformación Digital: sin fecha ni publicación oficial localizada; se declara de observancia para las dependencias y a la vez guía de referencia, y no fija plazo de reporte.
- **Oaxaca**, [Manual de Políticas de Seguridad de la Información](#) (2018, revisión de 2020): políticas obligatorias y auditoría externa anual del sistema de gestión, que no equivale a una certificación; se basa en ISO/IEC 27001:2005, edición ya sustituida, y su vigencia no está confirmada.

Ningún instrumento estatal identificado fija un plazo en horas para reportar incidentes; el de datos personales se está borrando

Ningún instrumento estatal vigente identificado obliga a notificar incidentes de ciberseguridad a una autoridad en un plazo en horas, y ninguna ley ni reglamento estatal revisado nombra ISO/IEC 27001 ni NIST. Conviene separar tres figuras que a menudo se confunden:

- 1. **Notificación de incidentes a una autoridad.** Federal: incidentes críticos en 24 horas o menos, solo para la APF. Estatal: por ley, solo Morelos, que obliga a sus dependencias a notificar "de inmediato" a la Agencia cualquier incidente o vulnerabilidad, bajo responsabilidad administrativa (art. 116); además, "de manera inmediata" en los instrumentos del Ejecutivo de Querétaro y la Ciudad de México, "a la brevedad posible" en Michoacán y sin plazo en Quintana Roo.
- 2. **Informe posterior de acciones correctivas.** Sonora, art. 130 de su Reglamento, con el plazo supletorio de diez días hábiles del art. 3.
- 3. **Aviso de vulneraciones de datos personales.** Es un deber distinto, que nace de la protección de datos y no cubre todo incidente de ciberseguridad.

El único plazo en horas que apareció fuera de los datos personales es de firma electrónica: el reglamento yucateco en la materia pide avisar en 24 horas cuando la clave privada sale de la custodia de su titular ([Digestum](#)). No es un régimen de incidentes. En las leyes revisadas, las remisiones más cercanas a un estándar son genéricas: "estándares internacionales" (Morelos, art. 17 fr. XXIX) y "mejores prácticas nacionales e internacionales" (Estado de México, art. 18; Tlaxcala, art. 46). De los revisados, solo dos instrumentos estatales del Ejecutivo nombran marcos: la guía de Quintana Roo, como referencia, y el manual de Oaxaca.

Las 72 horas se conservan en al menos cinco leyes no armonizadas

La LGPDPPSO de 2025, como la de 2017, ordena avisar las vulneraciones "sin dilación alguna" y no fija horas. Las 72 horas fueron un agregado de las leyes estatales de 2017, y las leyes armonizadas adoptan la fórmula general: Aguascalientes, por ejemplo, ya ordena informar "sin dilación alguna" (art. 29 de su ley de 2025) ([Congreso de Aguascalientes](#)).

Situación al corte (última versión localizada)	Entidades	N.º
Ley armonizada: "sin dilación alguna", sin plazo numérico	Aguascalientes, Baja California, Baja California Sur, Campeche, Chiapas, Ciudad de México, Colima, Durango, Estado de México, Michoacán, Nayarit, Oaxaca, Quintana Roo, Sonora, Tabasco, Tamaulipas, Tlaxcala, Veracruz y Zacatecas	19
Ley armonizada, artículo no leído	Puebla y Yucatán	2
Ley no armonizada que conserva 72 horas	Guanajuato (art. 56), Hidalgo (art. 57), Jalisco (art. 40), San Luis Potosí (art. 56) y Sinaloa (art. 50)	5

Situación al corte (última versión localizada)	Entidades	N.º
Ley no armonizada sin plazo numérico	Chihuahua, Coahuila, Guerrero, Nuevo León y Querétaro	5
No verificado	Morelos	1

Las 72 horas de Sinaloa se leyeron en una copia de Justia, y el listado oficial de su Congreso confirma que no hay una ley posterior a la de 2017; las de Guanajuato, Hidalgo, Jalisco y San Luis Potosí se cotejaron en las compilaciones oficiales de sus congresos o de su Ejecutivo ([Congreso de SLP](#)). Hidalgo (6-oct-2026) y Jalisco (15-jul-2026) ya aprobaron cambios cuya publicación no confirmamos. Cinco entidades pasaron a ley armonizada en el cotejo, todas con aviso "sin dilación": Veracruz (G.O.E. 30-jun-2025), Baja California Sur (B.O. 24-dic-2025), Nayarit (P.O. 1-jun-2026) y Campeche (P.O. 10-jun-2026), en su art. 34, y el Estado de México (Gaceta del Gobierno, 1-oct-2026), en su art. 36. Campeche y el Estado de México sustituyeron leyes que conservaban las 72 horas. Las cinco no armonizadas sin plazo numérico (Chihuahua, Coahuila, Guerrero, Nuevo León y Querétaro) se cotejaron en los portales de sus congresos, salvo Querétaro, cuyo portal no respondió; su versión de 2018 (última modificación 8-oct-2021) es la que reportaba vigente una entidad estatal al 31 de diciembre de 2025.

La operación puede ir por delante de la ley

El [ADEM-CERT](#), de la Agencia Digital del Estado de México, figura en el directorio de FIRST como equipo gubernamental desde el 27 de agosto de 2025. De los 33 equipos con país México registrados en FIRST al 22 de octubre de 2026, es el único de un gobierno estatal ([API de FIRST](#)); la lista de CSIRT Américas no se pudo leer. El Estado de México es apenas caso límite en el criterio normativo, y su Ley Orgánica de la Administración Pública (última reforma 1-oct-2026) no menciona a la Agencia ni la ciberseguridad: reparte el gobierno digital entre las secretarías General de Gobierno y de Finanzas (arts. 25 frs. XXVI y XXVII, y 29 frs. XLIII y XLIV) y la Oficialía Mayor (art. 59 fr. XXXII). Otras entidades tienen unidades de ciberseguridad que no son CSIRT registrados, como la Coordinación de Ciberseguridad de la Agencia de Tecnologías de Oaxaca o el Equipo de Seguridad de la STI de Querétaro. Morelos va más lejos en el papel: su ley ordena a la Agencia operar un Centro de Operaciones de Seguridad (art. 118), y el decreto que regula a la Agencia (P.O. 6572, 23-jun-2026) asigna su dirección a la Dirección General de Infraestructura Tecnológica. No localizamos evidencia pública de que ya opere.

Lo penal: verificado en cuatro entidades

Leímos el texto o el índice oficial del código penal solo en Jalisco (arts. 143-Bis y 143-Ter), Nayarit (art. 276 frs. II y XII), Puebla y Yucatán (Cap. V Ter, "Delitos informáticos"); en las otras 28 entidades lo penal no se evaluó de forma sistemática. El caso de Puebla es el que más se presta a confusión: la llamada "Ley de Ciberseguridad" de 2025 es una reforma al Código Penal. El 14 de abril de 2026, al resolver la acción de inconstitucionalidad 81/2025 y su acumulada 88/2025, la Suprema Corte invalidó el art. 480 (ciberasedio) por falta de taxatividad ([documento de la SCJN](#)). La invalidez prosperó en la acción de la CNDH (88/2025); la del PAN (81/2025) se desechó por falta de legitimación. La vigencia de los demás tipos de esa reforma no está verificada.

Sonora: deberes en su ley y su reglamento, y una iniciativa que los amplía

Sonora es fuerte por su ley y por su reglamento. La [Ley de Gobierno Digital](#) (Ley 173, B.O. 13-jun-2023) obliga a las dependencias y entidades del Ejecutivo; los otros poderes y los ayuntamientos solo se suman por adhesión, y la ley no usa la palabra "ciberseguridad".

La propia Ley 173 ya contiene un deber fuerte. Faculta a la Oficialía Mayor para emitir lineamientos y mecanismos de control "para la prevención, detección y corrección de incidentes de seguridad" (art. 71 fr. XVI) y obliga a los Entes a cumplirlos (art. 74 fr. IX); el incumplimiento genera responsabilidad administrativa (art. 84). Es la vía (e) del criterio. Esos lineamientos no los localizamos publicados: el Programa Especial de Gobierno Digital 2024-2027 los registró como pendientes. Cotejado contra el Boletín Oficial (Tomo CCXI, edición especial, 13-jun-2023) y contra el texto compilado del Congreso del Estado, que no registra reformas.

El detalle operativo está en el [Reglamento](#) (B.O. 11-jul-2024), cuyo capítulo "De la Seguridad de la Información" abarca los arts. 127 a 132:

- **Art. 127.** Los Entes "deberán establecer las medidas de seguridad que resulten necesarias" conforme a estándares de ciberseguridad que no nombra.
- **Arts. 128 y 129.** Extienden las medidas y el monitoreo de amenazas a los proveedores de herramientas tecnológicas.
- **Art. 130.** Tras una vulneración, exige entregar a la unidad de tecnologías coordinadora y a la Subsecretaría un informe detallado de acciones correctivas, sin plazo propio; aplica el genérico de diez días hábiles del art. 3.
- **Art. 131.** Ordena avisar "de manera inmediata" a los titulares de datos afectados.
- **Art. 83 fr. III.** Las propuestas de los proveedores deben incluir la obligación de "comunicar inmediatamente sobre posibles incidentes de seguridad": el deber llega al proveedor por contrato.

El Reglamento no prevé auditorías periódicas, capacitación obligatoria en seguridad ni un estándar con nombre. Alrededor de él hay planeación del Ejecutivo: la [Agenda Digital 2026](#) reporta como realizados en 2025 la autenticación de doble factor en portales, sistemas y correo, y programa para 2026 la autenticación multifactor y una política de contraseñas. Son acciones que declara el propio gobierno, sin verificación independiente. La Ley 82 de Protección de Datos Personales (B.O. 29-ago-2025) ya obliga a avisar vulneraciones "sin dilación alguna" (art. 34) y a capacitar al personal.

La iniciativa de Ley de Transformación Digital (Folio 04605)

Obtuvimos el texto por solicitud al Congreso del Estado el 22 de octubre de 2026. Es la iniciativa del gobernador Alfonso Durazo Montañón, fechada el 17 de septiembre de 2026 y remitida al Congreso por la Subsecretaría de Desarrollo Político el 5 de octubre (oficio SDP-00990/2026, Folio 04605). Expide la Ley de Transformación Digital, abroga la Ley 173 y la Ley de Mejora Regulatoria del Estado (transitorio Cuarto) y reforma y deroga fracciones del art. 23 Bis 2 de la Ley Orgánica del Poder Ejecutivo. Según su exposición de

motivos, el capítulo de ciberseguridad se revisó con apoyo técnico del Banco Interamericano de Desarrollo. Leímos el texto completo, un escaneo de 113 páginas, con reconocimiento óptico de caracteres. El Congreso la sometió a parlamento abierto, en el que Transformation Trends participa con propuestas (véase la declaración de interés).

En ciberseguridad (arts. 92 a 108), el texto de la iniciativa:

- **Fija un aviso de incidentes de máximo doce horas.** Las unidades de tecnologías de la información de cada Ente deben avisar a la Agencia "cualquier incidente de ciberseguridad" en un plazo no mayor a doce horas (art. 103 fr. X); las coordinadoras de sector, en el mismo plazo (art. 104 fr. IX), y los proveedores, por contrato, al área contratante (art. 106 fr. VI). Los servidores públicos deben informar "de manera inmediata" (art. 107 fr. VI), y la Agencia avisa a la Secretaría de Seguridad y Protección Ciudadana cuando el incidente lo amerite (art. 102 fr. XV).
- **Crea cinco inventarios estatales** (infraestructura, sistemas, dominios, identidades y proveedores con acceso; arts. 94 a 99), confidenciales en los supuestos y términos de las disposiciones aplicables (art. 94), y prohíbe operar infraestructura no registrada (art. 95).
- **Ordena controles mínimos obligatorios** por tipo de activo y criticidad, en lineamientos que emitirá la Agencia (art. 101), y doble factor en los sistemas internos con información sensible o crítica (art. 100 fr. III).
- **Obliga a los Entes a pactar con sus proveedores** cláusulas de seguridad, aviso de incidentes en doce horas, entrega íntegra al terminar, revocación de accesos y eliminación verificable de la información (art. 106). El deber del proveedor sigue siendo contractual, como hoy (Reglamento, art. 83), pero la ley fijaría su contenido mínimo.
- **Faculta a la Agencia** para verificar cuando lo determine, aprobar planes de remediación y ordenar la suspensión o baja de sistemas de riesgo crítico (art. 102 frs. IX, XII y XIII).
- **Mantiene las disposiciones reglamentarias vigentes**, es decir, el Reglamento de 2024, en lo que no se opongan y mientras se expiden las nuevas (transitorio Décimo; el nuevo Reglamento tendría 180 días hábiles, transitorio Tercero). El transitorio Décimo Segundo dice que la ausencia de lineamientos específicos no releva de cumplir la ley, pero lo plantea para interoperabilidad, centralización tecnológica y migración de sistemas.

Escenario que planteamos sin el texto	Lo que dice la iniciativa	Resultado en el radar
Se limita a principios y atribuciones de la Agencia	Impone deberes con verbo imperativo a Entes, unidades de tecnología y servidores públicos, y cláusulas obligatorias para proveedores (arts. 103 a 107)	No aplica
Conserva o amplía al menos un deber del criterio	Amplía la vía (b), aviso de incidentes, y la (e), lineamientos obligatorios (arts. 101 y 103)	Seguiría fuerte
Fija un plazo numérico para notificar incidentes	Doce horas (arts. 103 fr. X, 104 fr. IX y 106 fr. VI)	Primera ley estatal identificada con un plazo en horas para avisar incidentes de ciberseguridad

Escenario que planteamos sin el texto	Lo que dice la iniciativa	Resultado en el radar
Condiciona su aplicación a un reglamento futuro	El aviso en 12 horas, el doble factor y los inventarios no dependen de lineamientos; los controles mínimos sí (art. 101), y no tienen plazo de emisión	Parcialmente
Abroga la Ley 173 sin un transitorio que mantenga el Reglamento	Las disposiciones reglamentarias vigentes siguen en lo que no se opongan, mientras se expiden las nuevas (transitorio Décimo)	Atendido de forma transitoria, hasta el nuevo Reglamento

Lo que la iniciativa no trae. No define "incidente de ciberseguridad", y el aviso de doce horas aplica a cualquiera, sin graduarse por gravedad: la gravedad solo decide si la Agencia escala el caso a la Secretaría de Seguridad y Protección Ciudadana (art. 102 fr. XV). No fija plazo a la Agencia para emitir la política y los lineamientos de seguridad (solo el Reglamento tiene 180 días hábiles, transitorio Tercero). Prevé verificaciones basadas en riesgo cuando la Agencia lo determine, con facultad de requerir evidencias y de ordenar la suspensión de sistemas (art. 102 frs. IX, X y XIII), pero no auditorías periódicas ni simulacros. Tampoco designa un equipo de respuesta a incidentes (CSIRT): reparte la respuesta entre la Agencia, las coordinadoras de sector y los Entes (arts. 102 fr. XV, 104 y 105 fr. IX), y los avisos llegan a una "Mesa de Ayuda" que no define. Los ayuntamientos solo se suman por convenio (art. 2). Mientras no se apruebe, publique y entre en vigor, Sonora se clasifica por la Ley 173 y su Reglamento.

Sonora frente a los estados más avanzados

Comparamos a Sonora, hoy y con la iniciativa, con los cuatro estados de deberes o controles más concretos del radar: Morelos (único con aviso de incidentes por ley), la Ciudad de México y Querétaro (los instrumentos del Ejecutivo más completos) y Guerrero (auditorías por ley). Sumamos al Estado de México por su CSIRT registrado en FIRST, no por su marco normativo. Chiapas, Chihuahua y Tamaulipas también son fuertes, pero el instrumento del que depende su deber no aparece publicado; Michoacán tiene controles concretos en acuerdos del Ejecutivo, pero su ley es genérica.

Elemento	Sonora hoy	Sonora con la iniciativa	Morelos	Ciudad de México	Querétaro	Guerrero	Estado de México
Clasificación	Fuerte	Seguiría fuerte	Fuerte	Fuerte	Fuerte	Fuerte	Caso límite
Dónde está el deber	Ley 173 y Reglamento 2024	Capítulo propio en ley (arts. 92 a 108)	Ley (arts. 115 a 118)	Dos leyes y Lineamientos del Ejecutivo (2020)	Ley y Disposiciones del Ejecutivo (2025)	Ley 679	Ley de Gobierno Digital, ligada a portales
Aviso de incidentes a la autoridad	Sin aviso temprano; informe posterior a la Subsecretaría (plazo supletorio de 10 días hábiles)	12 horas, por ley	"De inmediato", por ley	"De manera inmediata", en lineamientos	"De manera inmediata", en disposiciones	No	No
Proveedores	Aviso inmediato, por contrato	Por contrato, con contenido mínimo fijado en ley: aviso en 12 horas, entrega y borrado (art. 106)	No identificado	No identificado	No identificado	No identificado	No identificado
Doble factor o multifactor	No en norma; el gobierno reporta doble factor	Obligatorio en sistemas internos con información sensible o crítica (art. 100)	No identificado	No identificado	Doble factor, en disposiciones	No identificado	No identificado
Auditoría, verificación o prueba	No	Verificación cuando la Agencia lo determine; sin auditoría periódica	Evaluación periódica de la Agencia	Auditoría al menos cada dos años	Plan de recuperación probado cada año	Auditoría al menos cada dos años	No

Elemento	Sonora hoy	Sonora con la iniciativa	Morelos	Ciudad de México	Querétaro	Guerrero	Estado de México
Monitoreo o respuesta (SOC o CSIRT)	No identificado	No designa un CSIRT; reparte la respuesta entre Agencia, coordinadoras y Entes	Centro de Operaciones de Seguridad (SOC), por ley	No identificado	Equipo de Seguridad, sin registro en FIRST	No identificado	ADEM-CERT, en FIRST
Inventarios de activos	No identificado	Cinco inventarios; no puede operar infraestructura no registrada	No identificado	No identificado	No identificado	No identificado	No identificado
Capacitación en seguridad	Solo en datos personales (Ley 82)	Programas, sin periodicidad	No identificado	Sí, en lineamientos	No identificado	No identificado	No identificado
Estándar internacional nombrado	No	No	Genérico ("estándares internacionales")	No	No	No	Genérico ("mejores prácticas")
Consecuencia por incumplir	Responsabilidad administrativa (art. 84)	Remite a la Ley de Responsabilidades (art. 123)	Responsabilidad administrativa (art. 116)	No identificado	No identificado	"Falta Grave" (art. 61, en reforma)	Sanciones de la ley (art. 77)

Con la iniciativa, Sonora sería la única entidad identificada con un plazo medible en ley para avisar incidentes de ciberseguridad y con un contenido mínimo fijado en ley para los contratos con proveedores; seguiría sin auditoría periódica obligatoria ni equipo de respuesta designado. Las doce horas serían el único plazo en horas para avisar incidentes de ciberseguridad a una autoridad entre las leyes estatales identificadas; las 72 horas que conservan cinco leyes se refieren a vulneraciones de datos personales. Morelos, por ley, y la Ciudad de México y Querétaro, en instrumentos del Ejecutivo, piden aviso "de inmediato": más exigente en el papel, pero sin un plazo que se pueda medir. La Política federal da hasta 24 horas a los incidentes críticos de la APF. Le faltaría lo que ya tienen otros: auditoría periódica por ley (la Ciudad de México y Guerrero, al menos cada dos años) y un equipo designado para responder a incidentes (Morelos prevé por ley un Centro de Operaciones de Seguridad y el Estado de México opera un CSIRT registrado en FIRST). Ninguna ley estatal revisada nombra un estándar internacional específico.

"No identificado" significa que no aparece en los instrumentos revisados para este radar, que no incluyó todos los acuerdos del Ejecutivo de cada estado. La columna de la iniciativa describe un texto que el Congreso aún no aprueba y que puede cambiar en el dictamen.

08

Las 32 entidades bajo el mismo criterio

Cada fila muestra el instrumento vigente que define la categoría y lo que se identificó alrededor de él. "No localizado" significa que no lo encontramos en las fuentes consultadas.

Entidad	Categoría	Instrumento vigente y disparador	Ejecutivo u operación	Agenda legislativa	Listado oficial	Confianza	Fuente
Aguascalientes	Genérico	Ley sobre el Uso de Medios y Actos Digitales y Electrónicos (P.O. 8-dic-2025): respaldo, recuperación y seguridad (art. 14)	Agenda Digital 2022-2027	No localizada	Búsqueda manual por palabras clave: sin otras leyes con deberes	Alta	SCJN
Baja California	Sin instrumento específico	Ley de Mejora Regulatoria (P.O. 30-dic-2022): solo la fórmula del expediente (art. 40)	No localizado	Reforma constitucional local presentada (may-2026, prensa)	Búsqueda manual por palabras clave: sin otras leyes con deberes	Media	Congreso

Entidad	Categoría	Instrumento vigente y disparador	Ejecutivo u operación	Agenda legislativa	Listado oficial	Confianza	Fuente
Baja California Sur	Sin instrumento específico	Ley sobre el uso de medios electrónicos y firma electrónica (2018): solo firma	No localizado	No localizada	Búsqueda manual por palabras clave: sin resultados	Baja	SFyA
Campeche	Sin instrumento específico	Ley de Firma Electrónica Avanzada y Uso de Medios Electrónicos (2014): solo firma	No localizado	No localizada	Completo	Media	Justia
Chiapas	Fuerte	Ley de Gobierno Digital (P.O. 19-mar-2025): Programa Anual de Ciberseguridad Gubernamental (arts. 9 fr. XVI, 24 y 25)	Sistema de Ciberseguridad Gubernamental (art. 14 fr. III); Programa no localizado	No localizada	Completo	Alta	Consejería Jurídica
Chihuahua	Fuerte	Ley de Gobierno Digital (P.O.E. 17-dic-2022): Programa de Seguridad Informática (arts. 22 fr. IX y 32)	Reglamento Interior de la Coordinación de Política Digital (2025); Programa no localizado	No localizada	Completo	Alta	Congreso
Ciudad de México	Fuerte	Ley de Operación e Innovación Digital (GOCDMX 31-dic-2018; últ. ref. 13-jul-2026), art. 32 fr. XIII; Ley de Ciudadanía Digital (GOCDMX 9-ene-2020; últ. ref. 13-jul-2026), art. 57. No revisada: Ley para el Desarrollo del Distrito Federal como Ciudad Digital y del Conocimiento (2012)	Lineamientos de Seguridad de la Información (2020)	Iniciativa del INFO CDMX (may-2025), sin dictamen	Búsqueda manual en el portal oficial	Alta	LOID
Coahuila	Genérico	Ley Sobre Gobierno Electrónico (P.O. 11-mar-2016): almacenamiento, respaldo y seguridad (art. 17)	No localizado	No localizada	Completo	Media	Congreso
Colima	Sin instrumento específico	Ley Sobre el Uso de Medios Electrónicos y Firma Electrónica (2009): solo firma. Ley Orgánica del Poder Ejecutivo y de la Administración Pública (últ. ref. 16-abr-2026): sin ciberseguridad; gobierno electrónico a cargo de Planeación, Finanzas y Administración (art. 35 fr. XVII)	Acuerdo del Registro Civil fundado en la LNETB (2025)	No localizada	Búsqueda manual por palabras clave: sin resultados	Media	Justia
Durango	Genérico	Ley del Gobierno Digital (2014): normas TI obligatorias sin objeto de seguridad (art. 16 fr. I)	No localizado	No localizada	Búsqueda manual por palabras clave: sin otras leyes con deberes	Alta	Congreso
Estado de México	Fuerte, caso límite	Ley de Gobierno Digital (últ. ref. 27-mar-2026): Estándares con "Administración de la seguridad" (arts. 19 fr. IX y 21; el deber de observarlos se ancla a los portales del art. 20). Ley Orgánica de la Administración Pública (últ. ref. 1-oct-2026): sin ciberseguridad	ADEM-CERT, en FIRST desde ago-2025	No localizada	Búsqueda manual por palabras clave: sin otras leyes con deberes	Media	IEEM

Entidad	Categoría	Instrumento vigente y disparador	Ejecutivo u operación	Agenda legislativa	Listado oficial	Confianza	Fuente
Guanajuato	Sin instrumento específico	Ley sobre el Uso de Medios Electrónicos y Firma Electrónica (2004): solo firma. Ley Orgánica del Poder Ejecutivo (últ. ref. 8-abr-2026): "normar y coordinar los servicios de informática" (art. 24 fr. VI inc. b), sin deberes de seguridad; "ciberseguridad" solo como capacidad de investigación de delitos de la Secretaría de Seguridad y Paz (art. 31 fr. V inc. g)	No localizado	Documentos aparecidos en búsqueda, no abiertos	Búsqueda manual por palabras clave: sin resultados	Media	Justia
Guerrero	Fuerte	Ley 679 de Gobernanza Digital (P.O. 29-dic-2023): auditorías al menos bienales (art. 55); "Falta Grave" (art. 61, en reforma)	Estrategia estatal de ciberseguridad no localizada	Reforma a los arts. 61 y 62 aprobada (sep-2026, prensa)	Completo	Alta	SCJN
Hidalgo	Sin instrumento específico	Mandato constitucional genérico (art. 3); ley de medios electrónicos y firma	No localizado	No localizada	Completo	Media	Congreso
Jalisco	Genérico	Ley Orgánica del Poder Ejecutivo: aprobar estándares de seguridad, sin declararlos obligatorios (art. 19 fr. XXXIII)	No localizado	Iniciativa de policía cibernética, sin aprobación localizada	Búsqueda manual por palabras clave: solo la ley de datos personales	Baja	Copia municipal
Michoacán	Genérico	Ley de Gobierno Digital (2021): "controles efectivos" (art. 11 fr. XV). Ley Orgánica de la Administración Pública (últ. ref. 8-mar-2025): sin ciberseguridad; la Secretaría de Finanzas y Administración coordina las TIC del gobierno (art. 19 fr. LXXIV)	Políticas Generales en Materia de Ciberseguridad (2024)	Documentos aparecidos en búsqueda, no abiertos	Búsqueda manual en el marco normativo del Congreso	Alta	COEAC
Morelos	Fuerte	Ley de Transformación Digital (POEM 6475, 3-oct-2025; texto original según la Consejería Jurídica): las dependencias deben notificar "de inmediato" a la Agencia todo incidente o vulnerabilidad, bajo responsabilidad administrativa (art. 116); Centro de Operaciones de Seguridad (art. 118)	Decreto que regula la Agencia de Transformación Digital (P.O. 6572, 23-jun-2026)	Controversia constitucional 273/2025; resolución no verificada en fuente primaria	Búsqueda manual en el Marco Jurídico estatal	Alta	SCJN
Nayarit	Fuerte, caso límite	Ley de Gobierno Digital (2022; últ. ref. 28-sep-2026): cumplir los Estándares (art. 23 fr. IV); rubro de seguridad opcional (art. 18 fr. VIII); protocolos obligatorios solo para registros con datos personales (art. 53)	Estándares no localizados	No localizada	Completo	Alta	Congreso
Nuevo León	Genérico	Ley sobre Gobierno Electrónico (2013): almacenamiento, respaldo y seguridad (art. 17)	Policía Cibernética (prensa)	Dos iniciativas de Ley de Ciberseguridad (2025), sin dictamen	Búsqueda manual por palabras clave: sin otras leyes con deberes	Media	Congreso

Entidad	Categoría	Instrumento vigente y disparador	Ejecutivo u operación	Agenda legislativa	Listado oficial	Confianza	Fuente
Oaxaca	Instrumento del Ejecutivo	Sin ley de gobierno digital identificada. Ley Orgánica del Poder Ejecutivo (últ. ref. P.O. 1-ago-2026): sin ciberseguridad ni seguridad de la información; solo atribuciones generales de tecnologías de la información (art. 46 fr. XXXIV Bis)	Manual de Políticas de Seguridad de la Información (2018; vigencia no confirmada)	No localizada	Búsqueda manual por palabras clave: sin otras leyes con deberes	Baja	Manual
Puebla	Genérico	Ley de Gobierno Digital (2015): "uso seguro" ligado a datos personales (art. 51); medidas "recomendadas" (art. 54)	Acuerdo de simplificación (2025), sin ciberseguridad	No localizada	Completo	Media	Justia
Querétaro	Fuerte	Ley de Gobierno Digital (2022): estándares mínimos de seguridad obligatorios (arts. 11 y 12 fr. IX)	Disposiciones TIC (jul-2025)	No localizada	No leído	Media	Querétaro Digital
Quintana Roo	Instrumento del Ejecutivo	Sin ley de gobierno digital; ley de medios electrónicos y firma. Ley Orgánica de la Administración Pública (últ. ref. 20-mar-2026): la Agencia de Transformación Digital emite directrices de gobierno digital que "deberán aplicar" las dependencias (art. 43 fr. LIV), sin mencionar la seguridad	Guía de Ciberseguridad (sin fecha); Decreto de la Agencia (nov-2025); Políticas Internas de Ciberseguridad de la propia Agencia (en su sitio desde sep-2026; no leídas)	No localizada	Búsqueda manual por palabras clave: solo la ley de medios electrónicos y firma (últ. ref. 16-jul-2021)	Media	Guía
San Luis Potosí	Sin instrumento específico	Sin ley de gobierno digital en el listado; acuerdo de 2016 sobre seguridad informática de vigencia no verificada	—	Iniciativa ciudadana de 2020, sin movimiento desde ago-2021	Completo	Media-baja	Acuerdo
Sinaloa	Genérico	Ley de Gobierno Electrónico (2016): "controles efectivos" (art. 20 fr. VIII)	No localizado	No localizada	Completo	Media	Copia
Sonora	Fuerte	Ley 173 de Gobierno Digital (B.O. 13-jun-2023): arts. 71 fr. XVI y 74 fr. IX; Reglamento (B.O. 11-jul-2024): arts. 3, 83 fr. III y 127 a 132	Lineamientos de incidentes no localizados; Agenda Digital 2026 (planeación)	Iniciativa de Ley de Transformación Digital (Folio 04605, 5-oct-2026): aviso de incidentes en 12 horas (art. 103 fr. X)	No leído	Alta	B.O.
Tabasco	Fuerte, caso límite	Ley de Gobierno Digital y Firma Electrónica (últ. ref. 24-dic-2025): arts. 18 fr. VIII, 22 fr. IV y 47 Novodecies	Agenda Digital Tabasco 2030, sin sección de ciberseguridad	No localizada	Completo	Alta	Congreso
Tamaulipas	Fuerte	Ley Orgánica de la Administración Pública (P.O. 18-ago-2026): art. 42 Bis frs. IV y V	Normas de seguridad no localizadas	No localizada	Completo	Alta	P.O.
Tlaxcala	Fuerte, caso límite	Ley de Gobernanza Digital (P.O. 3-oct-2023): arts. 67 fr. V y 69 fr. X; declaratoria no localizada	Simulacros a cargo de la Agencia (art. 88 fr. I)	No localizada	Búsqueda manual por palabras clave: sin otras leyes con deberes	Alta	Consejería Jurídica
Veracruz	Sin instrumento específico	Ley 563 de Firma Electrónica Avanzada (2015): solo firma. Ley Orgánica del Poder Ejecutivo (últ. ref. 15-may-2026): sin ciberseguridad; la Contraloría define la política de gobierno digital (art. 34 fr. XL)	Comisión de Simplificación y Digitalización (2026, prensa)	No localizada	Búsqueda manual por palabras clave: sin leyes con deberes de ciberseguridad	Media	Justia

Entidad	Categoría	Instrumento vigente y disparador	Ejecutivo u operación	Agenda legislativa	Listado oficial	Confianza	Fuente
Yucatán	Sin instrumento específico	Ley sobre el Uso de Medios Electrónicos y Firma Electrónica (2009)	Centro de Innovación Tecnológica con atribuciones de propuesta	No localizada	Completo	Media	Código Penal
Zacatecas	Sin instrumento específico	Ley de Firma Electrónica (2013): solo firma	No localizado	No localizada	Completo	Media	Congreso

09

Conclusión y límites

La pregunta "¿qué estados tienen ley de ciberseguridad?" tiene hoy una respuesta corta y poco informativa: ninguno identificado. La línea que divide a las entidades es si la ley impone deberes a los sujetos y si el instrumento que ordena existe. En cinco de los ocho casos fuertes plenos no localizamos ese instrumento, y en tres de ellos el deber depende de él; los controles más concretos viven en acuerdos del Ejecutivo, y el único CSIRT estatal en FIRST pertenece a una entidad que en el plano normativo es caso límite.

Al mismo tiempo, la armonización con la LGPDPSO está borrando el plazo en horas más extendido en las leyes estatales, las 72 horas para avisar vulneraciones de datos personales, sin que ninguna ley estatal identificada haya creado un plazo en horas para incidentes de ciberseguridad. Entre los instrumentos revisados, el único plazo de ese tipo es federal y solo obliga a la APF. Sonora podría ser la primera entidad identificada con ese plazo en ley: su iniciativa de Ley de Transformación Digital propone doce horas para avisar incidentes, aunque sin definir qué es un incidente.

El titular "ninguna ley identificada" se sostiene como afirmación sobre las fuentes revisadas, no sobre el universo normativo. Quedaron sin verificar:

- El listado oficial de leyes de Querétaro, cuyo portal no respondió el 22 de octubre, y el de Sonora.
- La resolución de la controversia constitucional 273/2025 (Morelos) en fuente primaria.
- La declaratoria del transitorio Primero de la Ley de Gobernanza Digital de Tlaxcala.
- El texto publicado de la reforma a los arts. 61 y 62 de la Ley 679 de Guerrero.
- Si Sonora ya emitió los lineamientos de incidentes del art. 71 fr. XVI de la Ley 173.
- La publicación de las reformas de datos personales aprobadas en Hidalgo y Jalisco.
- El articulado de las iniciativas de Ley de Ciberseguridad de Nuevo León y la Ciudad de México, que conocemos por comunicados y prensa.

10

Fuentes principales

Las fuentes de cada entidad están en la tabla de las 32 entidades. Marco federal y Sonora:

- [Ley Nacional para Eliminar Trámites Burocráticos](#), Cámara de Diputados; transitorios leídos en [mley.mx](#)
- [Decreto de reforma a los arts. 25 y 73 constitucionales](#), DOF 15-abr-2025
- [Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados](#)
- [Ley General de Archivos](#)
- [Ley Federal de Protección de Datos Personales en Posesión de los Particulares](#)
- [Ley General del Sistema Nacional de Seguridad Pública](#)
- [Acuerdo que emite la Política General de Ciberseguridad para la APF y texto de la Política \(ATDT\)](#)
- [Lineamientos para la implementación del modelo nacional](#), ATDT
- [Aviso sobre el Pacto Nacional para la Implementación de la LNETB](#), DOF 28-sep-2026
- [Iniciativa de Ley General para la Coordinación de la Ciberseguridad](#), Gaceta Parlamentaria 7-ene-2026
- [Directorio de FIRST: ADEM-CERT](#)
- Sonora: [Ley 173 de Gobierno Digital](#); [Reglamento](#) y [copia del Supremo Tribunal de Justicia](#); [Agenda Digital 2026](#); [Programa Especial de Gobierno Digital](#); [Ley 82 de Protección de Datos Personales](#); [Ley 85 de Prevención de Delitos Cibernéticos](#)
- Cobertura de la compilación privada usada donde no se leyó el listado oficial: [Justia](#), [índice de Morelos](#)
- Sonora: Iniciativa con proyecto de Ley de Transformación Digital y decreto que reforma y deroga diversas disposiciones de la Ley Orgánica del Poder Ejecutivo, Folio 04605 (oficio SDP-00990/2026, 5-oct-2026), obtenida por solicitud al Congreso del Estado el 22-oct-2026

CONTACTO

Transformation Trends

Capacitación y certificaciones en ciberseguridad, seguridad de la información e inteligencia artificial.
PECB Authorized Partner · EC-Council Accredited Training Center (ATC).

CONTACTO

Marcela Mexía

WHATSAPP

644 110 2672

CORREO

mm@transformationtrends.mx

SITIO

transformationtrends.com

