ELEVAN Cyber

ANÁLISIS REGIONAL 2026

REPORTE DE INCIDENTES DE CIBERSEGURIDAD EN AMÉRICA LATINA

¿Qué organizaciones están obligadas a reportar, ante qué autoridad y en qué plazo?

México Chile Argentina Uruguay Colombia Perú Ecuador

NO TODOS LOS PAÍSES TIENEN EL MISMO MODELO

En la región conviven tres enfoques:

OBLIGACIÓN HORIZONTAL

Aplica a entidades públicas y empresas privadas de sectores esenciales. El régimen más amplio.

OBLIGACIÓN PARA EL SECTOR PÚBLICO

Aplica principalmente a organismos gubernamentales. El alcance privado depende de la contratación o regulación específica.

OBLIGACIÓN SECTORIAL

Depende del sector regulado, especialmente servicios financieros. No existe una regla única para todas las organizaciones.

Esta comparación se concentra en incidentes de ciberseguridad. No incluye obligaciones derivadas exclusivamente de normas de protección de datos personales.

🇨🇱

CHILE

el régimen más amplio de la región

NORMATIVA

Ley N.º 21.663 — Ley Marco de Ciberseguridad
Decreto Supremo N.º 295 — Reglamento de Reporte de Incidentes

¿QUIÉNES DEBEN REPORTAR?

Órganos de la Administración del Estado e instituciones que presten servicios esenciales. Los Operadores de Importancia Vital (OIV) tienen responsabilidades reforzadas. Incluye:

- energía y combustibles
- telecomunicaciones
- transporte
- seguridad social
- servicios postales
- agua y saneamiento
- infraestructura digital
- banca y medios de pago
- salud
- industria farmacéutica

¿DÓNDE? & ¿EN QUÉ PLAZO?

Ante la **ANCI** vía CSIRT Nacional.

- Alerta temprana: **máximo 3 horas** desde que se toma conocimiento
- Luego: informes sucesivos exigidos por el reglamento

IDEA CLAVE

Chile establece una obligación transversal para entidades públicas y empresas privadas de servicios esenciales.



URUGUAY

reporte obligatorio a CERTuy

NORMATIVA

Ley N.º 20.212 · Decreto N.º 66/025

¿QUIÉNES DEBEN REPORTAR?

Sujetos obligados clasificados por AGESIC. También deben reportar:

- CSIRT sectoriales
- Centros de Operaciones de Seguridad (SOC)
- Entidades responsables de activos o servicios críticos, según su clasificación

¿QUÉ DEBEN REPORTAR?

- La ocurrencia de incidentes de ciberseguridad
- Potenciales incidentes que cumplan los criterios de CERTuy (comunicación inmediata)

¿DÓNDE? & ¿EN QUÉ PLAZO?

Ante el **CERTuy** — Centro Nacional de Respuesta a Incidentes de Seguridad Informática.

- **Dentro de las 24 horas** desde que se toma conocimiento del incidente

IDEA CLAVE

La obligación depende del perfil y la clasificación asignada por AGESIC, no solamente del sector económico de la entidad.



ARGENTINA

obligación centrada en el Sector Público Nacional

NORMATIVA

Decisión Administrativa N.º 641/2021
Disposición N.º 7/2021 de la Dirección Nacional de Ciberseguridad

¿QUIÉNES DEBEN REPORTAR?

Entidades y jurisdicciones del Sector Público Nacional (art. 8, inc. a), Ley N.º 24.156). Los proveedores pueden quedar alcanzados cuando la obligación sea incorporada normativa o contractualmente.

¿QUÉ DEBEN REPORTAR?

- Incidentes de seguridad que se hayan producido en el organismo
- Incidentes que puedan potencialmente producirse

¿DÓNDE? & ¿EN QUÉ PLAZO?

Ante la **Dirección Nacional de Ciberseguridad** o la autoridad que la sustituya.

- **Dentro de las 48 horas** desde que se toma conocimiento de la ocurrencia o potencial ocurrencia

IDEA CLAVE

No es una obligación horizontal para todas las empresas privadas argentinas. Su alcance confirmado se concentra en el Sector Público Nacional.

COLOMBIA

reporte según la gravedad del incidente

NORMATIVA

Resolución N.º 500/2021 — MinTIC · Decreto N.º 88/2022
Modelo de Seguridad y Privacidad de la Información (MSPI)

¿QUIÉNES DEBEN REPORTAR?

- Entidades públicas del orden nacional y territorial
- Sujetos obligados por la Política de Gobierno Digital
- Prestadores de servicios ciudadanos digitales

¿QUÉ Y DÓNDE?

- Incidentes **Muy Graves y Graves** : CSIRT Gobierno (entidades nacionales y territoriales)
- Otros sujetos: ColCERT cuando corresponda; puede intervenir un CSIRT sectorial
- Incidentes Menos Graves y Menores: comunicar una vez gestionados (fines estadísticos)

¿EN QUÉ PLAZO?

- Incidentes Graves o Muy Graves: **máximo 24 horas** después de su detección

IDEA CLAVE

La clasificación realizada por el responsable de seguridad digital determina la urgencia y el flujo de reporte.



MÉXICO

obligaciones sectoriales, no una regla única

NORMATIVA

No existe una ley federal única. Las responsabilidades se encuentran en disposiciones sectoriales, principalmente financieras.

¿QUIÉNES DEBEN REPORTAR? (EJEMPLO: IFPE)

Instituciones de Fondos de Pago Electrónico reguladas por la Ley Fintech y sus disposiciones secundarias. Otros tipos de entidades financieras tienen obligaciones propias.

¿QUÉ DEBEN REPORTAR?

- Incidentes que afecten la operación de la institución
- Eventos que comprometan fondos o servicios de clientes
- Situaciones que afecten proveedores, contrapartes u otras entidades del sistema financiero

¿DÓNDE? & ¿EN QUÉ PLAZO?

- Ante Banco de México y/o CNBV según el tipo de entidad
- Aviso inicial: **inmediatamente** ; información detallada: conforme a la regulación aplicable

IDEA CLAVE

En México debe identificarse primero el tipo exacto de entidad regulada. No existe un plazo único aplicable a todas las empresas.

PERÚ

un centro nacional, pero sin plazo general único

NORMATIVA

D. Leg. N.º 1412 — Ley de Gobierno Digital · D. de Urgencia N.º 007-2020
Marco de Confianza Digital y normas complementarias

¿QUIÉNES DEBEN REPORTAR?

Las entidades públicas gestionan y coordinan incidentes dentro del sistema nacional. El canal nacional también recibe reportes de:

- Empresas privadas, organizaciones y ciudadanos

¿QUÉ DEBEN REPORTAR?

- Incidentes que afecten sistemas, redes y servicios digitales
- Eventos que comprometan activos de información o continuidad operativa

¿DÓNDE? & ¿EN QUÉ PLAZO?

Ante el **CNSD** — Centro Nacional de Seguridad Digital — vía formulario oficial o incidentes@cnsd.gob.pe

- Sin plazo nacional único: el reporte debe efectuarse oportunamente, conforme al procedimiento institucional

IDEA CLAVE

Perú cuenta con una autoridad y un canal nacional definidos, pero no con un plazo horizontal equivalente al de Chile o Uruguay.



ECUADOR

gestión obligatoria, reporte externo sectorial

NORMATIVA

Acuerdo Ministerial MINTEL-2024-0003 · EGSI v3.0
Normas Superintendencia de Bancos · Política Nacional de Ciberseguridad

¿QUIÉNES DEBEN GESTIONAR O REPORTAR?

- Instituciones de la Administración Pública obligadas a implementar el EGSI
- Entidades controladas por la Superintendencia de Bancos
- Organizaciones sujetas a regulación sectorial

¿DÓNDE?

- Sector público: mecanismos internos y gubernamentales establecidos
- Sector financiero: instancias internas y Superintendencia de Bancos cuando la normativa lo requiera
- EcuCERT reconocida como instancia nacional de coordinación

¿EN QUÉ PLAZO?

- Sin plazo externo único: depende del sector, nivel de gravedad y organismo de control

IDEA CLAVE

Ecuador exige procesos formales de identificación, registro, escalamiento y respuesta, pero no presenta un plazo nacional uniforme de reporte externo.

COMPARACIÓN REGIONAL

¿Quién debe reportar y en cuánto tiempo?

PAÍS	ALCANCE PRINCIPAL	AUTORIDAD	PLAZO
Chile	Entidades públicas y prestadores de servicios esenciales	ANCI / CSIRT Nacional	**3 horas**
Uruguay	Sujetos obligados clasificados por AGESIC	CERTuy	**24 horas**
Argentina	Sector Público Nacional	Dir. Nacional de Ciberseguridad	**48 horas**
Colombia	Entidades públicas y sujetos de Gobierno Digital	CSIRT Gobierno / ColCERT	**24 h (Graves)**
México	Entidades reguladas por sector	Banco de México / CNBV	**Inmediato***
Perú	Principalmente entidades públicas	CNSD	*Sin plazo único*
Ecuador	Sector público y entidades reguladas	EcuCERT / supervisor sectorial	*Sin plazo único*

** México: en determinados sectores regulados; no existe un plazo único aplicable a todas las empresas.*

LA REGIÓN NO TIENE UN MODELO UNIFORME

- **Chile** tiene el régimen más amplio y estructurado, con el plazo más corto de la región (3 horas).
- **Uruguay** establece un reporte nacional obligatorio basado en perfiles y clasificación de entidades.
- **Argentina y Colombia** concentran sus obligaciones generales en el sector público.
- **México y Ecuador** funcionan principalmente mediante regulación sectorial; no hay plazo único.
- **Perú** cuenta con una autoridad nacional de coordinación, pero sin plazo general único confirmado.

LA PREGUNTA CORRECTA NO ES SOLO CUÁNTO TIEMPO TENGO PARA REPORTAR.

TAMBIÉN DEBEMOS PREGUNTAR:

01 ¿Qué tipo de organización soy?

02 ¿En qué sector opero?

03 ¿Cómo se clasifica el incidente?

04 ¿Qué autoridad tiene competencia?

05 ¿Existen obligaciones simultáneas ante distintos organismos?

ELEVAN
Cyber

ELEVANCYBER.COM

POWERING THE FUTURE OF CYBERSECURITY

Identificamos, aceleramos y escalamos la nueva generación de líderes en ciberseguridad.

USA MEXICO COLOMBIA ECUADOR PERU CHILE URUGUAY ARGENTINA BRAZIL