RED IBEROAMERICANA DE PROTECCION DE DATOS

Red Iberoamericana
Rede Ibero-Americana

Protocolo estándar regional de respuesta a vulneraciones de seguridad de los datos personales

Una aproximación desde la protección de datos personales

*Autor: Luis García Balcarce**

Elaborado en el marco de la Convocatoria "Trabajar en Red" 2025-2026

Septiembre 2026.

Publicado con el apoyo de la Agencia Española de Cooperación Internacional para el Desarrollo AECID

**"Las opiniones, análisis y conclusiones expresados en este documento pertenecen exclusivamente a su autor en calidad de experto independiente y no reflejan necesariamente la postura o criterio de la Red Iberoamericana de Protección de Datos (RIPD). Esta publicación no implica la aprobación de su contenido ni representa la posición institucional de la RIPD, la cual no se hace responsable del uso que pueda darse a la información aquí expuesta."*

Sumario ejecutivo

Este documento propone un protocolo regional de respuesta a vulneraciones de seguridad de los datos personales, concebido desde la protección de datos y no desde la ciberseguridad. La diferencia no es terminológica, ya que el eje de la respuesta no es el activo informático comprometido, sino la persona titular de los datos y la afectación que el incidente puede producir sobre sus derechos.

El protocolo está anclado en los Estándares de Protección de Datos de los Estados Iberoamericanos, en su versión aprobada el 26 de mayo de 2026, y toma como base el Estándar 22, complementado por el principio de seguridad del Estándar 21. No sustituye los marcos nacionales de ciberseguridad, con los que debe articularse, ni constituye un manual de gestión técnica de incidentes.

El diagnóstico comparado releva una muestra no exhaustiva de jurisdicciones iberoamericanas y revela heterogeneidad en cuatro variables: el plazo de notificación a la autoridad, el momento desde el cual ese plazo se computa, el umbral que activa el deber de notificar y el deber de comunicar a las personas afectadas. Los plazos van de las cuarenta y ocho horas a los quince días hábiles, y varios ordenamientos optan por fórmulas abiertas. El riesgo para los derechos y libertades es el umbral más extendido entre los marcos analizados.

Sobre esa base, el documento organiza la respuesta en ocho fases, de la preparación previa a la revisión posterior, con la evaluación del riesgo como fase nuclear. Esa evaluación se apoya en siete factores estructurados y ubica el incidente en uno de tres niveles. Sin riesgo: se documenta. Riesgo: se notifica a la autoridad. Alto riesgo: además se comunica a las personas afectadas. Toda vulneración se registra, incluso la no notificada, con la motivación de la decisión adoptada.

El protocolo propone contenidos mínimos homogéneos para la notificación a la autoridad y para la comunicación a las personas, define el rol de la autoridad de protección de datos en la recepción y gestión del incidente, y desarrolla cuatro instrumentos de cooperación regional. A falta de una autoridad principal con competencia vinculante en el espacio iberoamericano, se plantea un modelo de coordinación voluntaria que no desplaza la competencia de cada autoridad sobre los titulares de su jurisdicción.

Cierran el documento cuatro supuestos de casuística ilustrativa, una lista de verificación operativa para las primeras horas y un conjunto de recomendaciones regionales orientadas a una definición común de vulneración, un umbral anclado en el riesgo, la convergencia de plazos, la homogeneización de contenidos, el deber de registro, la articulación con los equipos nacionales de respuesta a incidentes, la protección reforzada de grupos vulnerables y la cooperación en el marco de la RIPD.

1. Introducción y propósito

Las vulneraciones de seguridad de los datos personales constituyen hoy uno de los riesgos más frecuentes y de mayor impacto sobre los derechos y libertades de las personas en la región. Su tratamiento suele abordarse predominantemente desde una óptica técnica -de ciberseguridad, infraestructura o ingeniería de sistemas-, en la que el eje de la respuesta es la integridad del sistema afectado. El presente documento propone una mirada distinta y complementaria: un protocolo de respuesta concebido desde la protección de datos personales, cuyo eje no es el activo informático comprometido, sino la persona titular de los datos y la afectación que el incidente puede producir sobre sus derechos fundamentales.

Este enfoque importa por una razón práctica. La pregunta técnica *¿qué sistema falló y cómo se restablece?* no coincide necesariamente con la pregunta jurídica que ordena el régimen de protección de datos: *¿qué información sobre qué personas quedó expuesta, qué riesgo genera ello para sus derechos y qué obligaciones de notificación, comunicación y documentación se activan en consecuencia?*. Un incidente puede estar técnicamente contenido y, aun así, requerir notificación a la autoridad y comunicación a las personas afectadas; y a la inversa, una falla de seguridad seria puede no constituir una vulneración relevante en términos de protección de datos. El protocolo busca precisamente ordenar esa segunda lógica.

El documento se inscribe en el marco de los **Estándares de Protección de Datos de los Estados Iberoamericanos**, cuya versión vigente fue aprobada el 26 de mayo de 2026, y toma como anclaje normativo regional su Estándar 22, relativo a la notificación de vulneraciones a la seguridad de los datos personales, complementado por el principio de seguridad del Estándar 21[1]. Se nutre, además, de la metodología internacional consolidada en materia de notificación de brechas y de las soluciones adoptadas por distintos ordenamientos de la región, sin pretender uniformar sus particularidades, sino ofrecer una base común de referencia que cada autoridad y cada legislación nacional pueda adoptar y adaptar.

No se trata, por tanto, de un manual de gestión técnica de incidentes ni de un sustituto de los marcos de ciberseguridad nacionales, con los que el protocolo debe articularse. Es un instrumento orientado a la capa de protección de datos: definiciones comunes, criterios de evaluación del riesgo para los derechos de las personas, umbrales y plazos de notificación, contenidos mínimos, deberes de documentación y pautas para la actuación de las autoridades de protección de datos y su cooperación regional.

[1] RIPD, Estándares de Protección de Datos de los Estados Iberoamericanos, aprobados el 26 de mayo de 2026 (Cartagena de Indias), Estándar 22 (Notificación de vulneraciones a la seguridad de los datos personales) y Estándar 2.1.s (definición).

2. Marco conceptual desde la protección de datos

2.1. Vulneración de seguridad: el concepto que ordena el protocolo

Los Estándares Iberoamericanos definen la vulneración de la seguridad de los datos personales como toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o el acceso no autorizados a dichos datos. Esta definición, coincidente en lo sustancial con la del artículo 4(12) del RGPD, es deliberadamente amplia y se centra en el **efecto sobre los datos**, con independencia del vector técnico que lo haya producido (un ciberataque, un error humano, la pérdida de un soporte físico o una configuración deficiente).

Antes de seguir avanzando, conviene distinguir el **incidente de seguridad** de la **vulneración relevante en términos de protección de datos**. Todo evento adverso que comprometa la seguridad de la información es un incidente; pero solo se convierte en una cuestión de protección de datos cuando afecta, o razonablemente puede afectar, datos personales. Un incidente que no involucra datos personales, o que recae sobre datos efectivamente anonimizados, queda fuera del ámbito de este protocolo, sin perjuicio de su tratamiento por los marcos de seguridad de la información correspondientes.

2.2. Tipología funcional: confidencialidad, integridad y disponibilidad

Desde la perspectiva de protección de datos, las vulneraciones se clasifican funcionalmente según el atributo de seguridad comprometido, la denominada tríada CIA[2], criterio que resulta más útil para evaluar el riesgo que la categorización técnica del ataque:

- **Vulneración de confidencialidad:** acceso o divulgación no autorizados a los datos personales (por ejemplo, filtración de información en un ataque, o envío erróneo de datos a un destinatario equivocado).

- **Vulneración de integridad:** alteración no autorizada de los datos, que afecta su exactitud o veracidad (por ejemplo, modificación indebida de registros).

- **Vulneración de disponibilidad:** pérdida de acceso a los datos o su destrucción, sea de forma permanente o temporal (por ejemplo, cifrado por ransomware o borrado sin copia de respaldo recuperable).

[2] EDPB, Guidelines 9/2022 on personal data breach notification under the GDPR, v2.0, adoptadas el 28 de marzo de 2023.

Un mismo incidente puede comprometer simultáneamente más de un atributo. Algunos ordenamientos de la región han incorporado, además, la autenticidad como cuarto atributo. Esta clasificación orienta la evaluación del riesgo, porque cada tipo de vulneración proyecta consecuencias distintas sobre las personas afectadas.

2.3. El criterio rector: el riesgo para los derechos y libertades de las personas

La nota distintiva del protocolo es que la decisión de notificar y comunicar no depende de la gravedad técnica del incidente, sino del riesgo que este genera para los derechos y libertades de las personas titulares. Este es el criterio que articula todo el ciclo de respuesta y el que, en última instancia, justifica la intervención de la autoridad de protección de datos. La sección 6 desarrolla los factores que permiten estimar ese riesgo de manera estructurada.

3. Diagnóstico regional

Los marcos analizados presentan un grado significativo de heterogeneidad en el tratamiento de las vulneraciones de seguridad. Las diferencias no son menores y se concentran en cuatro variables: el plazo de notificación a la autoridad, el momento desde el cual ese plazo se computa (dies a quo), el umbral que activa el deber de notificar y el deber de comunicar a las personas afectadas. El cuadro siguiente sintetiza a título comparativo, algunos de los modelos vigentes y los estándares de referencia. Las jurisdicciones relevadas constituyen una muestra no exhaustiva del espacio iberoamericano. Las conclusiones de esta sección se refieren a esa muestra.

Marco / jurisdicción	Plazo a la autoridad	Cómputo del plazo	Umbral de notificación	Comunicación a las personas
Estándares RIPD (2026)	Sin dilación alguna	Desde el conocimiento por el responsable	Salvo que, tras evaluarla, no genere riesgo para los derechos y libertades	Cuando conlleve alto riesgo, sin dilación indebida
RGPD / UE (referencia)	72 horas	Desde el conocimiento	Salvo improbabilidad de riesgo	Sin dilación indebida si hay alto riesgo
Argentina (Ley 25.326)	Sin deber general expreso	-	El proyecto de reforma de la LPDP incorpora el deber de notificación	Previsto en el proceso de reforma
Brasil (Res. CD/ANPD n.º 15/2024)	3 días hábiles, salvo que la legislación específica establezca un plazo de notificación distinto. Para los agentes de tratamiento de	Desde el momento en que el responsable del tratamiento tenga conocimiento de que el incidente ha	Riesgo o daño relevante a los titulares	3 días hábiles a los titulares afectados

Marco / jurisdicción	Plazo a la autoridad	Cómputo del plazo	Umbral de notificación	Comunicación a las personas
	pequeño porte, este plazo será el doble.	afectado a datos personales.		
Chile (Ley 21.719)	Por los medios más expeditos posibles y sin dilaciones indebidas (vigencia dic. 2026)	Desde el conocimiento	Riesgo razonable para los derechos y libertades de los titulares (art. 14 sexies, inc. 1º)	Cuando afecte datos sensibles, de NNA o de carácter económico/financiero
Colombia (Ley 1581/2012)	15 días hábiles (reporte al RNBD/SIC)	Desde la detección o conocimiento	Incidente que comprometa la información personal (reforma estatutaria en trámite)	No prevista de forma general en la norma vigente
Ecuador (LOPDP 2021)	Máximo 5 días (art. 43 LOPDP)	Desde que el responsable tuvo conocimiento de la vulneración	Vulneración de seguridad con riesgo (notificación también al organismo de regulación y control competente y al CSIRT correspondiente, estos últimos para fines informativos y de coordinación técnica)	Cuando exista riesgo para los derechos y libertades, dentro de los 3 días desde que se tuvo conocimiento del riesgo, con las excepciones legalmente previstas (art. 46 LOPDP)
El Salvador (LPDP, art. 25)	72 horas	Desde que el responsable tiene conocimiento de la vulneración	Conocimiento de la vulneración de seguridad, sin umbral de alto riesgo	A los titulares afectados dentro del mismo plazo, sin condicionarla al alto riesgo; en ese plazo se notifica también a la ACE y a la FGR
México (LFPDPPP 2025)	De forma inmediata	Desde el conocimiento	Afectación a derechos patrimoniales o morales	A los titulares afectados, de inmediato
Perú (Regl. DS 016-2024-JUS)	48 horas	Desde el conocimiento o detección	Incidente de seguridad (a los titulares, solo si afecta sus derechos)	48 horas, en lenguaje claro, si afecta sus derechos
Uruguay (Decreto 64/020)	Mitigación dentro de las 24 horas y comunicación a la URCDP dentro de las 72 horas	Desde que se constata la vulneración	Sin umbral cuantitativo: basta que incida en la protección de datos	De inmediato a quienes sufran afectación significativa
Andorra (Ley 29/2021)	Sin dilación indebida y, si es posible, 72 horas como máximo	Desde que el responsable tiene constancia de la vulneración	Salvo improbabilidad de riesgo para los derechos y libertades	Cuando pueda acarrear riesgo alto

La muestra analizada indica que los marcos relevados atraviesan un momento de convergencia acelerada: en poco más de un año se han renovado o estrenado marcos en varios de los Estados analizados -la ley salvadoreña vigente desde noviembre de 2024, el reglamento peruano vigente desde marzo de 2025, la reforma ecuatoriana del artículo 43 de la LOPDP por la Ley Orgánica para el Fortalecimiento de la Ciberseguridad de mayo de 2026, la nueva ley mexicana de 2025 y la ley chilena que entrará en vigor a fines de 2026-, todos los cuales incorporan, con distinta intensidad, el deber de notificar las vulneraciones. Del cuadro se desprenden tres lecciones para el diseño de un estándar regional.

Primera, sobre los plazos. El abanico es notablemente amplio: desde las 48 horas (Perú) y las 72 horas (Andorra, El Salvador, Uruguay y el marco europeo de referencia), pasando por los tres días hábiles (Brasil) y los cinco días (Ecuador), hasta los quince días hábiles para el reporte al registro nacional (Colombia); en el otro extremo, varios ordenamientos optan por fórmulas abiertas -de forma inmediata, sin dilación o por los medios más expeditos (México, Chile y el propio Estándar 22)[3]. Esta dispersión, que en los marcos analizados va de dos días a tres semanas hábiles, es el principal obstáculo para una respuesta regional homogénea.

Segunda, sobre el cómputo. El dies a quo tampoco es uniforme: mientras la mayoría de los marcos analizados lo fija en la detección o el conocimiento del incidente, Brasil lo difiere hasta la confirmación de que los datos personales resultaron efectivamente afectados, lo que altera de modo sustantivo el plazo real disponible[4]. A ello se añade la variedad de umbrales: desde la ausencia de umbral cuantitativo (Uruguay) hasta criterios anclados en el riesgo para los derechos y libertades (Andorra, Chile, Ecuador), en el riesgo o daño relevante a los titulares (Brasil) o en la afectación de derechos determinados (México, Perú). Las categorías de datos especialmente protegidas operan en Chile como umbral de la comunicación a los titulares, no de la notificación a la Agencia[5]. El Salvador adopta la solución inversa: el artículo 25 de la LPDP impone notificar a la autoridad y a los titulares afectados dentro del mismo plazo de 72 horas, sin condicionar la comunicación a un umbral de alto riesgo. La dispersión es menor en este punto, ya que el riesgo para los derechos y libertades es el umbral más extendido entre los marcos analizados.

Tercera, sobre la dimensión institucional. La identidad y el diseño de la autoridad receptora también varían entre los marcos analizados: junto a autoridades especializadas de creación reciente conviven autoridades de competencia amplia. En Ecuador, tras la reforma del artículo 43 de la LOPDP por el artículo 14 de la Ley Orgánica para el Fortalecimiento de la Ciberseguridad, publicada en el Quinto Suplemento del Registro Oficial Nº 290, de 22 de mayo de 2026, una misma vulneración puede activar la notificación a la autoridad de protección de datos personales, al organismo de regulación y control competente y al CSIRT correspondiente, estos dos últimos para fines informativos y de coordinación

[3] Uruguay, Ley N.º 19.670 (arts. 37 a 40) y Decreto N.º 64/020, arts. 3 y 4: mitigación dentro de las 24 horas y comunicación a la URCDP dentro de las 72 horas de conocida la vulneración.
[4] Brasil, ANPD, Resolução CD/ANPD n.º 15, de 24 de abril de 2024 (Regulamento de Comunicação de Incidente de Segurança), arts. 6, 9 y 10; LGPD (Lei 13.709/2018), art. 48.
[5] Colombia, Ley 1581/2012 y Circular Única de la SIC (reporte de incidentes al RNBD dentro de los 15 días hábiles); Ecuador, LOPDP (2021), Ley Orgánica de Ciberseguridad y normativa de la SPDP (2025); Perú, Reglamento de la Ley 29733 aprobado por Decreto Supremo N.º 016-2024-JUS, art. 34 (vigente desde el 30/03/2025); Chile, Ley 21.719 (DO 13/12/2024), con entrada en vigor en diciembre de 2026.

técnica. ARCOTEL resulta destinataria cuando sea el organismo sectorial competente, no como receptora universal de toda vulneración. En El Salvador, la autoridad de control es la Agencia de Ciberseguridad del Estado, y la misma vulneración se notifica además a la Fiscalía General de la República, lo que suma al mapa institucional una autoridad de ciberseguridad con competencia en protección de datos y una intervención del Ministerio Público.

4. Principios rectores del protocolo

La respuesta a una vulneración debe ordenarse en torno a un conjunto de principios que, derivados de los Estándares Iberoamericanos, dan coherencia a cada fase del ciclo:

- **Centralidad de la persona.** El criterio que gobierna toda decisión es el riesgo para los derechos y libertades de las personas titulares, no la gravedad técnica del incidente.

- **Responsabilidad proactiva y demostrada.** La capacidad de responder no se improvisa: se prepara, se documenta y se puede acreditar ante la autoridad.

- **Enfoque basado en el riesgo.** La intensidad de las medidas y de los deberes de notificación es proporcional al riesgo estimado.

- **Oportunidad.** La utilidad de la respuesta depende de su prontitud; la demora reduce la posibilidad de mitigar el daño.

- **Minimización del daño.** La primera obligación es limitar la afectación a las personas, antes incluso que el restablecimiento operativo.

- **Transparencia y lealtad.** La comunicación a las personas afectadas debe ser veraz, comprensible y útil, en lenguaje claro y sencillo.

- **Trazabilidad y documentación.** Toda vulneración, incluso la no notificada, se registra para que la decisión adoptada sea reconstruible y justificable.

- **Cooperación.** La gestión articula a responsables, encargados, autoridades de protección de datos y, cuando corresponda, equipos nacionales de respuesta a incidentes, sin confundir sus roles.

5. El ciclo de respuesta

El protocolo organiza la respuesta en ocho fases. Aunque se presentan de forma secuencial, en la práctica se solapan: la contención puede iniciarse antes de completar la evaluación del riesgo, y la documentación acompaña a todas las etapas. El acento de cada fase está puesto en lo que la protección de datos exige, no en la operación técnica subyacente.

Fase 0. Preparación

La respuesta efectiva presupone una preparación previa. Desde la protección de datos, ello implica al menos: la existencia de un punto de responsabilidad claro -idealmente el delegado u oficial de protección de datos como punto de contacto-; un procedimiento interno escrito de gestión de vulneraciones; un registro de tratamientos que permita identificar con rapidez qué datos y qué personas pueden verse afectados; cláusulas contractuales con los encargados que fijen el deber de comunicar sin dilación al responsable; y formación periódica del personal para reconocer y escalar incidentes.

Fase 1. Detección y registro inicial

Desde el momento en que el responsable -o el encargado, que debe avisar sin dilación- toma conocimiento de un posible incidente, se abre el procedimiento y se efectúa un registro inicial: fecha y hora de conocimiento, descripción preliminar de los hechos, tratamientos potencialmente involucrados y persona responsable de la gestión. Este registro es relevante porque, en varios ordenamientos, marca el inicio del cómputo de los plazos.

Fase 2. Contención y mitigación

La primera prioridad es limitar la afectación a las personas. Sin entrar en el detalle técnico -que corresponde a las áreas de seguridad-, desde la protección de datos interesa verificar que se adopten medidas idóneas para detener la exposición de los datos y reducir el daño potencial (por ejemplo, revocar accesos indebidos, recuperar o invalidar información, o impedir su ulterior difusión). Algunos ordenamientos fijan un plazo breve y específico para iniciar estas medidas de mitigación.

Fase 3. Evaluación del riesgo para los derechos y libertades

Es la fase nuclear del protocolo y la que determina las obligaciones posteriores. Consiste en estimar, con la información disponible, el nivel de riesgo que el incidente genera para las personas afectadas, a partir de los factores que se desarrollan en la sección 6. El resultado de esta evaluación ubica el incidente en uno de tres niveles -sin riesgo, riesgo o alto riesgo- de los que dependen, respectivamente, la mera documentación interna, la notificación a la autoridad y la comunicación a las personas.

Fase 4. Notificación a la autoridad de protección de datos

Cuando la evaluación arroja que la vulneración genera un riesgo para los derechos y libertades, el responsable la notifica a la autoridad de protección de datos. La notificación debe practicarse con prontitud y admite carácter **escalonado**: si no se dispone de toda la información, se efectúa una notificación inicial y se completa de manera fundamentada en un momento posterior. Los contenidos mínimos se detallan en la sección 7.

Fase 5. Comunicación a las personas afectadas

Cuando la vulneración conlleva un alto riesgo para los derechos y libertades, además de notificar a la autoridad, el responsable comunica el incidente a las personas afectadas, sin dilación indebida, en lenguaje claro y sencillo. El objetivo de esta comunicación no es meramente informativo: busca habilitar a la persona para que adopte medidas de autoprotección. Su contenido se detalla en la sección 7.

Fase 6. Documentación y registro de vulneraciones

El responsable documenta toda vulneración ocurrida en cualquier fase del tratamiento, incluso aquellas que, por no superar el umbral de riesgo, no se notifican. El registro debe contener, como mínimo, los hechos relacionados con la vulneración, sus efectos, la evaluación del riesgo realizada, la decisión de notificar o no -con su motivación- y las medidas correctivas adoptadas. Esta documentación es la base de la rendición de cuentas y debe estar a disposición de la autoridad. Diversos ordenamientos fijan, además, plazos mínimos de conservación del registro.

Fase 7. Revisión y mejora

Resuelto el incidente, corresponde un análisis posterior orientado a extraer lecciones: identificar la causa raíz desde la perspectiva del tratamiento de datos, evaluar la eficacia de la respuesta y actualizar las medidas de seguridad, los procedimientos y la formación. Esta fase cierra el ciclo y alimenta la Fase 0 de futuros incidentes.

6. Evaluación del riesgo para las personas

La evaluación del riesgo es un ejercicio estructurado, no intuitivo. Aunque cada incidente es singular, conviene apoyarse en un conjunto estable de factores que la metodología internacional ha consolidado[6]. Ninguno de ellos es decisivo por sí solo: el riesgo resulta de su combinación.

6.1. Factores de evaluación

Factor	Consideraciones desde la protección de datos
Tipo de vulneración	Confidencialidad, integridad o disponibilidad -o su combinación-; cada tipo proyecta consecuencias distintas.
Naturaleza y sensibilidad de los datos	Los datos sensibles o de categorías especiales (salud, biométricos, genéticos, neurodatos, ideología, orientación sexual, entre otros) elevan el riesgo de modo significativo.
Volumen de datos y número de personas	El alcance cuantitativo incide, aunque un incidente que afecte a pocas personas con datos muy sensibles puede ser de alto riesgo.
Facilidad de identificación	Cuán sencillo resulta atribuir los datos a una persona concreta; la seudonimización o el cifrado robusto pueden reducir el riesgo.
Gravedad de las consecuencias	Posibilidad de daños como suplantación de identidad, fraude, pérdida económica, discriminación, daño reputacional o afectación física o psíquica.
Características de las personas	La afectación de niñas, niños y adolescentes o de personas en situación de vulnerabilidad agrava el riesgo y exige responsabilidad reforzada.
Permanencia y reversibilidad	Si el efecto es transitorio y reversible, o permanente; si los datos pueden recuperarse o la difusión revertirse.

6.2. Niveles de riesgo y consecuencias

La combinación de los factores anteriores permite ubicar el incidente en uno de tres niveles, cada uno con consecuencias jurídicas precisas:

Nivel	Descripción	Consecuencia
Sin riesgo	La vulneración no genera, tras su evaluación, riesgo para los derechos y libertades (p. ej.,	No se notifica. Se documenta internamente, con la motivación de la decisión.

[6] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches (2013), que propone estimar la gravedad en función del contexto del tratamiento, la facilidad de identificación y las circunstancias del incidente.

Nivel	Descripción	Consecuencia
	datos ya públicos o efectivamente cifrados e inaccesibles).	
Riesgo	La vulneración puede afectar los derechos y libertades de las personas.	Se notifica a la autoridad de protección de datos. Se documenta.
Alto riesgo	La vulneración puede producir consecuencias graves o de difícil reversión para las personas.	Se notifica a la autoridad y se comunica a las personas afectadas. Se documenta.

La evaluación se realiza con la información disponible en cada momento y puede revisarse a medida que se conocen nuevos hechos; una recalificación al alza del nivel de riesgo activa las obligaciones correspondientes.

7. Contenido mínimo de las notificaciones

Para facilitar la adopción regional y la cooperación entre autoridades, conviene homogeneizar los contenidos mínimos de las dos comunicaciones que el protocolo prevé. Las siguientes pautas, derivadas del Estándar 22 y de la práctica internacional, pueden servir como plantilla de referencia.

7.1. Notificación a la autoridad de protección de datos

- Naturaleza de la vulneración, incluyendo, cuando sea posible, las categorías y el número aproximado de personas y de registros afectados.
- Tipo de vulneración según la tríada (confidencialidad, integridad y/o disponibilidad).
- Datos de contacto del delegado u oficial de protección de datos o del punto de contacto donde obtener más información.
- Posibles consecuencias de la vulneración para las personas afectadas.
- Medidas adoptadas o propuestas por el responsable para remediar la vulneración y, en su caso, para mitigar sus posibles efectos negativos.
- Cuando proceda, indicación de si la notificación es inicial o complementaria, y de la información pendiente.

7.2. Comunicación a las personas afectadas

Redactada en lenguaje claro y sencillo, evitando tecnicismos, debe contener al menos:

- La naturaleza del incidente.
- Los datos personales comprometidos.
- Las acciones correctivas realizadas de forma inmediata.
- Recomendaciones concretas sobre las medidas que la persona puede adoptar para proteger sus intereses (por ejemplo, cambiar credenciales o extremar la atención ante intentos de fraude).
- Los medios disponibles para obtener mayor información y asistencia.

8. El rol de la autoridad de protección de datos

El protocolo no se agota con quien trata los datos. La autoridad de protección de datos cumple un papel activo en la gestión del incidente, que conviene ordenar para garantizar previsibilidad y trato equivalente en la región.

8.1. Recepción y gestión de la notificación

1. **Recepción y acuse.** Disponer de un canal estable y accesible de recepción de notificaciones, con acuse y registro del incidente.
2. **Triaje.** Clasificar el incidente según el riesgo declarado y la información disponible, priorizando los de alto riesgo y los que afecten a grupos vulnerables.
3. **Requerimiento de información.** Solicitar, en cualquier momento, información adicional o complementaria al responsable.
4. **Coordinación.** Articular, cuando corresponda, con los equipos nacionales de respuesta a incidentes (CSIRT/CERT) y otras autoridades sectoriales, sin asumir funciones técnicas que no le competen y preservando su rol de garante de los derechos.
5. **Supervisión y, en su caso, medidas correctivas o sancionatorias.** Evaluar la adecuación de la respuesta del responsable y ejercer sus potestades de supervisión, corrección y sanción conforme a la legislación nacional.

6. **Comunicación pública.** Cuando el interés de las personas afectadas lo justifique, recomendar o requerir la difusión del incidente, o informar a la ciudadanía con pautas de autoprotección.

8.2. Cooperación regional

Las vulneraciones rara vez respetan fronteras, un mismo encargado puede tratar datos de personas de varios Estados, y un incidente puede tener efectos transnacionales. Para evitar tanto la duplicación de cargas sobre los responsables como los vacíos de competencia entre autoridades, conviene promover mecanismos estables de cooperación.

Los Estándares Iberoamericanos de 2026 reconocen la cooperación internacional entre autoridades de control como uno de sus objetivos, y la RIPD cuenta con la arquitectura institucional para articularla: una Secretaría Permanente, un Comité Ejecutivo integrado por varias autoridades y un Plan Estratégico 2026-2030 que ubica la intersección entre inteligencia artificial y protección de datos y la protección de colectivos vulnerables entre sus prioridades. Sobre esa base, un protocolo regional de incidentes puede traducirse en instrumentos concretos.

El primero es una red permanente de puntos de contacto, esto implica un directorio actualizado de enlaces de respuesta a incidentes en cada autoridad, con disponibilidad para casos urgentes, que evite que la cooperación dependa de canales informales o de relaciones personales. El segundo es un formato común de notificación, entendido como una plantilla regional interoperable que recoja un núcleo mínimo de información -naturaleza del incidente, categorías y volumen de datos y de titulares afectados, riesgos y medidas adoptadas-, de modo que un responsable que opera en varios Estados pueda cumplir ante distintas autoridades sin reconstruir la información cada vez, y que las autoridades puedan compararla. Que sea interoperable no implica que sea idéntica, ya que cada autoridad conserva sus requisitos propios. El tercero son criterios compartidos de evaluación del riesgo, con orientaciones comunes sobre cuándo un incidente alcanza el umbral de "riesgo" o de "riesgo alto", para que un mismo hecho no reciba tratamientos divergentes según la frontera. Y el cuarto son mecanismos de asistencia mutua, que permitan a una autoridad requerir o prestar apoyo en la investigación de incidentes con efectos en su territorio cuando el responsable está establecido en otro Estado.

A diferencia del modelo europeo de ventanilla única, el espacio iberoamericano no cuenta con una autoridad principal con competencia vinculante sobre las demás, por lo que ante determinados casos se podría aplicar un modelo de coordinación voluntaria que ante un incidente que afecte a titulares de varios Estados, las autoridades involucradas pueden designar de común acuerdo una autoridad coordinadora que centralice el intercambio y evite requerimientos redundantes al responsable, sin que ello desplace la competencia de cada autoridad sobre los titulares de su propia jurisdicción.

La cooperación debe articularse, además, con el plano de la ciberseguridad. Muchos incidentes activan en paralelo a las autoridades sectoriales y a los equipos de respuesta a incidentes. Conviene por ello tender puentes con las redes de CSIRT y los foros de ciberseguridad de la región, delimitando con claridad que esa coordinación tiene finalidad técnica de contención y no traslada la tutela del derecho ni la potestad sancionadora, que permanecen en la autoridad de protección de datos.

Por último, dado que buena parte de los grandes responsables y encargados opera globalmente y muchos incidentes tienen origen o efectos fuera del espacio iberoamericano, es prudente mantener canales con marcos y autoridades externos.

Toda esta cooperación exige salvaguardas. El intercambio de información sobre incidentes debe contar con base jurídica suficiente y respetar la confidencialidad y la minimización, porque la información de un incidente puede contener, en sí misma, datos personales o secretos comerciales. La cooperación no debe convertirse en una nueva fuente de riesgo, y debe preservar en todos los casos la competencia y la independencia de cada autoridad. El objetivo es coordinar, no crear una competencia supranacional.

9. Hacia un estándar regional de plazos

La diversidad de plazos descrita en el diagnóstico es el principal obstáculo para una respuesta regional coherente. Sin desconocer el derecho interno de cada Estado, el protocolo propone un modelo de referencia que armoniza las soluciones existentes y resulta compatible con la fórmula abierta del Estándar 22. El parámetro que sigue constituye una propuesta de armonización regional. No sustituye los términos legalmente establecidos y vigentes en cada Estado, que continúan rigiendo en sus respectivas jurisdicciones:

- **Notificación a la autoridad:** sin dilación indebida y, como referencia máxima orientativa, dentro de las 72 horas de conocida la vulneración. Este parámetro concilia las soluciones de los ordenamientos analizados y de los marcos internacionales y ofrece un horizonte temporal predecible.

- **Cómputo:** desde que el responsable toma conocimiento de la vulneración, sin diferir el inicio del plazo a la confirmación completa de sus efectos, lo que se compensa con la admisión de notificaciones escalonadas.

- **Notificación escalonada:** posibilidad de una comunicación inicial completable de manera fundamentada en un plazo posterior razonable, cuando no se disponga de toda la información.

- **Comunicación a las personas:** sin dilación indebida cuando exista alto riesgo, priorizando la utilidad de la información para la autoprotección.

- **Registro:** conservación de la documentación de toda vulneración por un plazo mínimo razonable y uniforme en la región, que permita la supervisión posterior por la autoridad.

10. Vulneraciones en entornos de inteligencia artificial

El uso de sistemas de inteligencia artificial no crea un régimen distinto de respuesta a vulneraciones. Sí introduce supuestos de hecho que el protocolo debe poder clasificar con las categorías ya definidas.

Tres situaciones merecen atención. La primera son los conjuntos de datos de entrenamiento: su exposición, extracción o alteración constituye una vulneración de confidencialidad o de integridad, y el riesgo debe evaluarse sobre las personas cuyos datos integran el conjunto, aunque el tratamiento haya tenido una finalidad de desarrollo. La segunda son los errores de procesamiento automatizado que alteran datos personales o los asignan a la persona equivocada: configuran vulneraciones de integridad, y el riesgo se agrava cuando la salida del sistema condiciona el acceso a un derecho o a un servicio. La tercera es la cadena de proveedores: el entrenamiento, el alojamiento y la inferencia suelen estar distribuidos entre varios encargados, por lo que el deber de aviso sin dilación al responsable debe quedar expresamente previsto en los contratos.

La evaluación del riesgo sigue los factores de la sección 6, con dos consideraciones adicionales. La dificultad de revertir la incorporación de datos a un modelo ya entrenado incide en el factor de permanencia y reversibilidad. Y la posibilidad de inferir atributos no declarados a partir de los datos comprometidos puede elevar el riesgo por encima del que sugiere el conjunto expuesto.

11. Casuística ilustrativa

Los siguientes supuestos, anonimizados y de carácter general, muestran cómo el protocolo opera en la práctica. No describen casos reales ni de ningún Estado en particular.

11.1. Cifrado de bases por programa malicioso, sin copia recuperable

Vulneración de disponibilidad. Si los datos no pueden restaurarse desde una copia de respaldo, hay pérdida permanente de disponibilidad. Según la sensibilidad de los datos y las consecuencias para las personas (por ejemplo, imposibilidad de prestar un servicio esencial), el incidente puede alcanzar el nivel de alto riesgo y exigir comunicación a las personas afectadas, además de la notificación a la autoridad.

11.2. Envío de un correo con datos a un destinatario equivocado

Vulneración de confidencialidad. El riesgo depende de la naturaleza de los datos y de la posibilidad de revertir la divulgación (por ejemplo, confirmación de borrado por el destinatario). Un envío puntual de datos no sensibles, rápidamente revertido, puede no superar el umbral; un envío de datos sensibles a múltiples destinatarios, sí.

11.3. Pérdida de un dispositivo con datos cifrados

Si el cifrado es robusto y la clave no se ha visto comprometida, el riesgo para las personas puede ser bajo, de modo que el incidente se documente sin necesidad de notificación. La conclusión cambia si la clave se perdió o si el cifrado era débil.

11.4. Extracción de datos en un ataque dirigido

Vulneración de confidencialidad de alto riesgo cuando se extraen datos identificables, especialmente sensibles. Activa, por regla, tanto la notificación a la autoridad como la comunicación a las personas afectadas, con recomendaciones de autoprotección.

12. Lista de verificación operativa

Síntesis práctica para las primeras horas tras el conocimiento de una vulneración. Funciona como recordatorio de campo y no sustituye la evaluación del caso concreto.

- Registrar fecha y hora de conocimiento del incidente y abrir el expediente interno.
- Identificar qué tratamientos, qué datos y qué personas pueden estar afectados.
- Iniciar de inmediato las medidas para contener y mitigar la afectación a las personas.
- Clasificar el tipo de vulneración (confidencialidad, integridad, disponibilidad).
- Evaluar el nivel de riesgo conforme a los factores de la sección 6.
- Si hay riesgo, notificar a la autoridad de protección de datos dentro del plazo de referencia.
- Si hay alto riesgo, preparar y enviar la comunicación a las personas en lenguaje claro y sencillo.
- Documentar la evaluación, la decisión -notificar o no- y su motivación.
- Si el incidente se originó en un encargado, verificar que este haya cumplido su deber de aviso sin dilación.
- Tras la resolución, realizar el análisis de lecciones aprendidas y actualizar medidas y procedimientos.

13. Recomendaciones regionales

A modo de cierre, se proponen recomendaciones orientadas a fortalecer una respuesta regional armonizada, coherente con los Estándares Iberoamericanos y respetuosa del derecho interno de cada Estado.

1. **Adoptar una definición común de vulneración** de seguridad de los datos personales, tomando como base la del Estándar 22, para asegurar un punto de partida compartido.

2. **Anclar el deber de notificar en el riesgo** para los derechos y libertades de las personas, antes que en umbrales puramente cuantitativos o en la gravedad técnica del incidente.

3. **Converger hacia un plazo de referencia** de notificación a la autoridad -sin dilación indebida y como máximo orientativo 72 horas- notificaciones escalonadas y sin desplazar los plazos legalmente vigentes en cada Estado.

4. **Homogeneizar los contenidos mínimos** de las notificaciones a la autoridad y de las comunicaciones a las personas, mediante formatos comunes de referencia.

5. **Establecer el deber de registro de toda vulneración**, incluso de la no notificada, con un plazo mínimo de conservación uniforme.

6. **Articular la actuación de la autoridad con los equipos nacionales de respuesta a incidentes**, preservando el rol de garante de derechos de la primera.

7. **Reforzar la protección de grupos vulnerables**, en particular de niñas, niños y adolescentes, en la evaluación del riesgo y en la comunicación.

8. **Establecer criterios comunes para la evaluación del riesgo**, con orientaciones compartidas sobre cuándo un incidente alcanza el umbral de riesgo y el de alto riesgo, para que un mismo hecho no reciba tratamientos divergentes según la jurisdicción."

9. **Incorporar un enfoque preventivo y de gestión integral de las vulneraciones**, que abarque la preparación previa, la detección, la contención, la respuesta y la revisión posterior, y no se agote en el cumplimiento del deber de notificar."

10. **Fortalecer la trazabilidad y la preservación de la evidencia** del incidente desde su detección, en condiciones que permitan la supervisión posterior de la autoridad y, cuando corresponda, la actuación de otras instancias competentes."

11. **Desarrollar criterios específicos para vulneraciones de alcance transfronterizo**, que precisen qué autoridades se notifican, con qué información y bajo qué secuencia cuando el incidente afecta a titulares de más de un Estado.

12. **Promover, en el marco del Observatorio y la RIPD, mecanismos de cooperación regional**: puntos de contacto, criterios compartidos y canales de intercambio para incidentes de alcance transnacional, evitando la duplicación de cargas y los vacíos de competencia.

14. Referencias

1. RIPD, Estándares de Protección de Datos de los Estados Iberoamericanos, aprobados el 26 de mayo de 2026, Cartagena de Indias (en especial, Estándares 21 y 22 y la definición del Estándar 2.1.s).

2. RIPD, Estándares de Protección de Datos Personales para los Estados Iberoamericanos (2017), como antecedente.

3. European Data Protection Board (EDPB), Guidelines 9/2022 on personal data breach notification under the GDPR, versión 2.0, adoptadas el 28 de marzo de 2023.

4. Reglamento (UE) 2016/679 (RGPD), arts. 4(12), 33 y 34.

5. Consejo de Europa, Convenio 108+ para la protección de las personas con respecto al tratamiento de datos de carácter personal (modernizado), art. 7.

6. Uruguay, Ley N.º 19.670 (arts. 37 a 40) y Decreto N.º 64/020, de 17 de febrero de 2020.

7. Brasil, ANPD, Resolução CD/ANPD n.º 15, de 24 de abril de 2024 (Regulamento de Comunicação de Incidente de Segurança); LGPD (Lei 13.709/2018), art. 48.

8. Chile, Ley 21.719 que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (DO 13/12/2024; entrada en vigor en diciembre de 2026), art. 14 sexies.

9. Colombia, Ley Estatutaria 1581 de 2012 y Circular Única de la Superintendencia de Industria y Comercio (reporte de incidentes de seguridad al RNBD dentro de los 15 días hábiles).

10. Ecuador, Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en el Quinto Suplemento del Registro Oficial Nº 459, de 26 de mayo de 2021, arts. 43 y 46; su Reglamento General (2023); Ley Orgánica para el Fortalecimiento de la Ciberseguridad, publicada en el Quinto Suplemento del Registro Oficial Nº 290, de 22 de mayo de 2026, art. 14; y normativa de la Superintendencia de Protección de Datos Personales (SPDP), en particular la Resolución Nº SPDP-SPD-2026-0040-R, de 9 de septiembre de 2026, Norma Técnica de Notificaciones de Vulneraciones de la Seguridad de los Datos Personales.

11. México, Ley Federal de Protección de Datos Personales en Posesión de los Particulares (DOF 20/03/2025; vigente desde el 21/03/2025), art. 19.

12. Perú, Ley N.º 29733 y su Reglamento aprobado por Decreto Supremo N.º 016-2024-JUS (vigente desde el 30/03/2025), art. 34.

13. El Salvador, Ley para la Protección de Datos Personales, aprobada por Decreto Legislativo N.º 144, de 12 de noviembre de 2024, art. 25.

14. Andorra, Ley 29/2021, de 28 de octubre, cualificada de protección de datos personales, arts. 36 y 37.

15. Argentina, Ley 25.326 de Protección de los Datos Personales; recomendaciones de la AAIP y proceso de reforma de la LPDP.

16. ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches (2013).

17. ISO/IEC 27035 (gestión de incidentes de seguridad de la información) e ISO/IEC 29151 (protección de datos personales), como referencias técnicas complementarias.

18. RIPD, Orientaciones Específicas y Recomendaciones Generales para el tratamiento de datos en proyectos de inteligencia artificial (2019).