https://doi.org/10.18800/dys.202601.008

FECHA DE RECEPCIÓN: 10/11/2025
FECHA DE APROBACIÓN: 13/02/2026

Aplicación del Principio de Responsabilidad Demostrada frente a incidentes de seguridad en el tratamiento de datos personales: análisis de Colombia, Brasil, Perú y México

Application of the Accountability Principle to Personal Data Processing Security Incidents: A Comparative Analysis of Colombia, Brazil, Peru, and Mexico

Lina M. Díaz*
Universidad Externado de Colombia

Resumen:
El presente artículo examina cómo el Principio de Responsabilidad Demostrada (PRD) y el deber de seguridad, concebidos para una protección de datos práctica y actualizada, se ven afectados cuando un incidente de seguridad se considera automáticamente prueba de incumplimiento, generando un riesgo moral que desincentiva la inversión en prevención. Se propone que una evaluación adecuada del deber de seguridad, aplicando el PRD, requeriría que la Autoridad Nacional de Protección de Datos (ANPD) analice la evaluación de riesgos del Responsable, la idoneidad de las medidas de seguridad y su actuación post-incidente. El estudio de casos concretos en Colombia, Brasil, Perú y México revela una diversidad en la aplicación, con algunos casos donde la mera ocurrencia del incidente implica responsabilidad, y otros donde se realiza un análisis más profundo de las medidas implementadas. Finalmente, se plantea un análisis tripartito para considerar los ciberataques como eximentes de responsabilidad bajo ciertas circunstancias, buscando reconciliar el PRD con el deber de seguridad y fomentar una gestión de riesgos diligente.

Abstract:
This article examines how the Accountability Principle and the security obligation, both conceived to ensure practical and up-to-date personal data protection, are affected when the mere occurrence of a security incident is automatically treated as evidence of non-compliance, thereby creating a moral hazard that discourages investment in preventive measures. It argues that a proper assessment of the security obligation, consistent with the Accountability Principle, requires the National Data Protection Authority (DPA) to examine the controller's risk assessment, the appropriateness of the security measures implemented, and the controller's post-incident response. Drawing on case studies from Colombia, Brazil, Peru, and Mexico, the article identifies divergent approaches to enforcement. In some cases, the mere occurrence of a security incident is treated as sufficient to establish liability,

* Abogada de la Universidad Externado con Maestría en Propiedad Intelectual y Derecho de la Competencia de la London School of Economics (LSE) y Maestría en Economía Aplicada de la Universidad de los Andes. Cuenta con más de 7 años de experiencia en procesos administrativos y judiciales en materia de propiedad intelectual, protección de datos, protección al consumidor y derecho de la competencia.

whereas in others the authorities undertake a more thorough assessment of the safeguards implemented before determining whether the controller breached its legal obligations. Finally, the article proposes a three-part analytical framework under which cyberattacks may, in certain circumstances, constitute a defence against liability. This framework seeks to reconcile the Accountability Principle with the security obligation while promoting diligent, risk-based information security management.

Palabras clave:
Principio de Responsabilidad Demostrada – deber de seguridad – ciberseguridad – responsabilidad administrativa.

Keywords:
Accountability Principle – security obligation – cybersecurity – administrative responsibility.

1. Introducción

En materia de protección de datos personales, el Principio de Responsabilidad Demostrada (PRD, en adelante) implica que los Responsables deben gestionar activamente y estar en capacidad de demostrar que cumplieron con sus obligaciones en caso de ser requeridos por la Autoridad Nacional de Protección de Datos (ANPD, en adelante) o el Titular. Por su parte, el deber de seguridad implica adoptar medidas necesarias y efectivas para proteger los datos personales de los riesgos de acceso, uso o divulgación no autorizados. Estos principios se crearon con el objetivo de que la protección de los datos personales no se limitase a políticas que se ven muy bien en papel, sino que se llevara a un plano práctico y se actualizara conforme evoluciona la tecnología.

Por ello, teóricamente, el PRD exige que las obligaciones del Responsable y su cumplimiento se analicen a partir de una evaluación de los riesgos que implica el tratamiento; lo que determinará las medidas que deben adoptarse teniendo en consideración el tipo de datos tratados —sensibles o no—, el volumen de datos, los estándares técnicos vigentes, los recursos del Responsable, etc.

Sin embargo, en varios casos, el acaecimiento de un incidente de seguridad es considerado automáticamente como prueba del incumplimiento de los deberes y obligaciones del Responsable y, en consecuencia, sancionado. Esto se considera problemático porque genera un riesgo moral, en la medida en que desincentiva la adopción y mejora incremental de la seguridad y por el contrario estimula la inversión en seguros, notificaciones y contención del daño reputacional del Responsable en estos eventos. Esto es, un efecto opuesto a lo esperado por la norma. Adicionalmente, el castigo automático al Responsable por el incidente obvia que los ataques pueden ser imprevisibles e irresistibles configurando causales eximentes de responsabilidad.

Lo que acá se plantea es que una adecuada evaluación del deber de seguridad, en caso de un incidente de seguridad, en el que efectivamente se aplique el PRD, requeriría que la ANPD analice la evaluación de riesgos efectuada por el Responsable, determine si las medidas de seguridad eran acordes con el nivel de riesgo y, también, cómo actuó luego de ocurrido el incidente. Esto es, si notificó oportunamente a la autoridad, si correspondía informar a los Titulares, si adoptaron medidas efectivas para contener el ataque y correctivos adecuados para evitar que vuelva a presentarse. Este tipo de análisis, en lugar de la responsabilidad automática que actualmente opera en casos de incidentes, materializa el PRD al tiempo que evita el riesgo moral porque en algunos casos el Responsable podría evitar sanciones.

Para analizar esta problemática, este documento se divide en cuatro secciones. Las dos primeras abordan el origen y contenido del PRD y del deber de seguridad desde una perspectiva teórica para precisar el alcance de las obligaciones que conllevan sobre los Responsables. La tercera sección estudia casos de incidentes de seguridad en Colombia, Brasil, Perú y México para analizar la interacción práctica entre PRD y el deber de seguridad y plantea un análisis en tres niveles sobre la posibilidad de que los ciberataques eximan de responsabilidad administrativa al Responsable. La cuarta sección plantea, a modo de reflexión final para futuros desarrollos, el papel del Estado garante de la seguridad en este entorno. Finalmente se plantean algunas conclusiones.

2. Origen y aplicación del Principio de Responsabilidad Demostrada

El *Accountability Principle* o Principio de Responsabilidad Demostrada (PRD) surge de las Directrices sobre la protección de la privacidad y los flujos transfronterizos de datos personales de la OECD (OECD, 2002). Allí se estableció el PRD como un principio independiente, con el objetivo de que los demás principios y recomendaciones para la protección de datos personales tuvieran un efecto práctico y tangible que condujera a la adopción de medidas concretas; lo que además permitiría la transferencia internacional de datos.

Desde la primera mención por la OECD, se han realizado varios intentos por precisar el PRD y los criterios para determinar que en efecto un Responsable cumplió con la carga de demostrar que actuó diligentemente en el tratamiento de los datos en caso de ser llamado a rendir cuentas sobre su actividad (Alhadeff, 2012). Por ejemplo, el Marco de Privacidad de la APEC, los Proyectos Galway, París y Madrid, las Guías del Grupo de Trabajo del artículo 29, etc. De estos esfuerzos, surgieron parámetros que hoy sirven de guía tanto de las actividades que debe realizar el Responsable o Encargado y de lo que deben evaluar las ANPD. Tales parámetros incluyen prácticas como contar con una estructura organizacional que sea acorde con el tamaño y tipo de tratamiento que se realiza, contar con políticas para el tratamiento y mecanismos concretos de aplicación, capacitación y educación continua a quienes realicen el tratamiento, implementación de medidas técnicas de seguimiento y auditoría, evaluación de riesgos, etc. (Alhadeff, 2012).

El PRD tiene dos elementos, por un lado, la obligación de adoptar medidas apropiadas y efectivas para aplicar los requisitos y principios de la protección de datos y, por el otro, tener la capacidad de demostrar cómo se ha cumplido con los parámetros establecidos por la regulación (Alhadeff, 2012). Sin embargo, el PRD no es prospectivo por definición; es decir, no determina con precisión cuáles son esos mecanismos que el Responsable debe adoptar para demostrar que en efecto adoptó medidas para proteger los datos. Esto se debe a que, como está estructurado al menos en la *General Data Protection Regulation* (GDPR) europea, el PRD busca que los Responsables evalúen el riesgo de forma que puedan ponderar las ventajas del procesamiento frente al riesgo que implique para los derechos fundamentales de los Titulares y determinar qué medidas técnicas y organizacionales deben implementar para protegerlos (Quelle, 2018).

El PRD se estructuró así con el objetivo de que las normas sobre protección de datos personales tuviesen una verdadera aplicación práctica y su cumplimiento dejara de ser un mero formalismo (Alhadeff, 2012). Al imponer al Responsable la carga de evaluar los riesgos del tratamiento frente a los derechos del Titular para determinar e implementar las medidas que fuesen suficientes para mitigar esos riesgos y, además, ser capaz de demostrar que efectivamente se implementaron esas medidas, se buscaba que las normas de protección de los datos y la privacidad de los Titulares se materializaran. Esto porque el Responsable sabe que tendrá que rendir cuentas del procesamiento de forma que se anticipa y prepara para cumplir en debida forma con los requisitos legales (De Hert, 2022).

Aunque es cuestionable si esto realmente ha funcionado, considerando que en la mayoría de circunstancias los Titulares nos limitamos a "aceptar" las políticas de tratamiento y conceder todo tipo de autorizaciones sin siquiera leerlas, siempre que podamos generar imágenes con inteligencia artificial o crear una cuenta en una red social (Eurostat, 2024; McClain & Faverio, 2023; Quelle, 2018).

Ahora corresponde analizar cómo se aplica el PRD al evaluar si los Responsables cumplieron o no con sus deberes en el tratamiento. En teoría, el PRD impone dos elementos que deberían considerarse en este respecto. En primer lugar, se aplica cuando, por algún motivo, la autoridad competente o el Titular llaman al Responsable a rendir cuentas (*holds him acoountable*) sobre el tratamiento. En segundo lugar, implica que se analicen las medidas implementadas por el Responsable en consideración a varios elementos como: el tamaño de la empresa, la naturaleza del dato y el grado de afectación a los derechos del Titular en caso de un tratamiento inadecuado.

En Colombia, las dos instancias en que el Responsable puede ser llamado a rendir cuentas sobre el tratamiento de los datos son, por un lado, en el curso de una investigación administrativa iniciada de oficio o con motivo de una queja por parte de la ANPD —la Superintendencia de Industria y Comercio, en el caso colombiano— o por medio de una acción civil en la que solicite la declaración de incumplimiento de las obligaciones del Responsable y la correspondiente indemnización (*liability*). Aunque vale señalar que el proceso administrativo sancionatorio ante la ANPD en Colombia no tiene finalidades restaurativas pues esto escapa a las funciones de la ANPD (Decreto 4886 de 2011, articulo 17.4).

En el curso de cualquiera de esas dos instancias, debería tenerse en cuenta el tipo de obligaciones que imponen las leyes de protección de datos al Responsable y al Encargado, las cuales pueden ser tanto de resultado (tener prueba de la autorización para el tratamiento, por ejemplo) como de medio (implementar medidas razonables para informar al Encargado de que el Titular solicitó la actualización de sus datos) (Alsenoy, 2016). En ese sentido, la aplicación del PRD variará en cada caso porque en las obligaciones de resultado no bastará con que el Responsable pruebe haber adoptado mecanismos para solicitar la autorización para el tratamiento y así demostrar que cumplió con su obligación. En otros casos, sí debería bastar con probar que se adoptaron medidas dirigidas a cumplir con el deber legal, tomando en consideración lo ya dicho sobre el tamaño de la empresa, el nivel de riesgo al que se someten los derechos del Titular, etc. para que se tenga por cumplida la obligación.

En consecuencia, al menos en procesos administrativos, la aplicación del PRD conllevaría

a que, para evitar una condena, bastara con que el Responsable probara que cumplió o por lo menos que implementó los mecanismos adecuados para cumplir con sus obligaciones, según se trate de obligaciones de resultado o de medio.

Sin embargo, la doctrina reconoce que, si se ha generado daño al Titular, la prueba de diligencia o cuidado o de haber tomado medidas dirigidas a cumplir con la ley no debería impedir que el Titular sea debidamente reparado (Bennett, 2012). Por otro lado, Alsenoy (2016) señala que, bajo la General Data Protection Regulation (GDPR), los Responsables tienen el deber de reparar los daños que se causen en el procesamiento de los datos y que el régimen de responsabilidad jurídica es estricto (objetivo) porque una vez que se demuestra el incumplimiento de la ley en el procesamiento no puede escapar de su obligación de reparación señalando que no actuó con culpa o negligencia.

En el caso de los juicios de responsabilidad civil derivados de daños en el tratamiento de los datos personales (Alhadeff, 2012) señala que incluso los Titulares deberían estar amparados por figuras jurídicas como una presunción o la carga dinámica de la prueba (*proof proximity principle),* porque muchas veces el procesamiento de los datos se hace a puerta cerrada y los Titulares no tienen forma de probar que en efecto hubo un tratamiento inadecuado de los datos.

Entonces, podría decirse que en ambas instancias —el proceso administrativo o el judicial de responsabilidad civil— y ante los dos tipos de obligaciones —de medio o de resultado— el PRD tiene el efecto de invertir la carga de la prueba, de forma que corresponde al Responsable probar que cumplió ante la solicitud de la ANPD o del Titular. De esta forma, la autoridad y el Titular tienen una carga sencilla de acusar, de señalar que el Responsable no cumplió o adoptó las medidas adecuadas para cumplir con lo que señala la ley.

Ahora bien, en Colombia no hay un consenso respecto del régimen de responsabilidad que aplica a los Responsables, si es objetiva o subjetiva, pues no existe una norma precisa que regule este asunto (Tacha, 2024), a diferencia de otros países como Argentina y la Unión Europea. Tampoco existe consenso respecto del efecto del PRD en el sistema de atribución de responsabilidad de los Responsables. Unos señalan que el PRD estableció un deber de conducta cuyo incumplimiento implica negligencia, la cual puede ser muy difícil de probar sin los conocimientos técnicos adecuados, por lo que se justifica que se presuma la culpa por lo que el Responsable es el encargado de probar la ausencia de culpa (Tacha, 2024).

Mientas que otra parte de la doctrina argumenta que se trata de un sistema de responsabilidad objetiva por varias razones. De una parte, porque el tratamiento de datos personales comporta un riesgo, del que se benefician las empresas profesionales en la materia e implica un riesgo a los derechos fundamentales del Titular (Riaño, 2023). De otra parte, porque deben protegerse los intereses y derechos de personas que pueden encontrarse en situaciones de indefensión como los menores de edad y los consumidores (Riaño, 2023)[1].

Cabe señalar que esta discusión sobre el tipo de responsabilidad de los Responsables no es exclusiva de Colombia. En Estados Unidos, el deber de implementar medidas razonables de seguridad en el tratamiento de datos personales puede tener diferentes fuentes jurídicas como normas especiales, la responsabilidad derivada de la creación de un daño antijurídico (*tort* o negligencia) u obligaciones adquiridas contractualmente que imponen a una parte esta obligación. Sin embargo, no hay un criterio exacto para determinar la razonabilidad de las medidas de seguridad que deben adoptarse en cada caso de forma que al implementarles efectivamente se reduzca el riesgo de incumplir con tal obligación (Tschider, 2023).

De esta forma, se podría estar incentivando comportamientos que no incrementan la seguridad de los datos, creando un *moral hazard*. El Responsable o Encargado en vez de adoptar medidas de seguridad, al no tener la certeza de que con ello van a salir avante en un eventual juicio de responsabilidad pues no pueden saber si las medidas que adopten serán consideradas como razonables o no (Tschider, 2023), deciden entonces destinar sus recursos a pagar seguros, a notificar a los Titulares y a la ANPD en caso de un incidente de

1 Aunque el fundamento normativo difiere, en Colombia en los casos de fraude electrónico de información gestionada por los bancos se aplica un régimen de responsabilidad objetiva basado en la teoría de la creación y el aprovechamiento de una actividad que por sí misma es riesgosa. En ese sentido los bancos tienen una responsabilidad objetiva en caso de fraude de la que sólo podrán eximirse si demuestran culpa exclusiva de la víctima o fuerza mayor (Jiménez, 2025). Adicionalmente, hay otros motivos o justificaciones para que los bancos tengan este nivel de responsabilidad: i) los bancos tienen una posición de garantes de la seguridad de las operaciones electrónicas, ii) también tienen el control y la capacidad para implementar las medidas de seguridad, iii) los usuarios financieros no tienen la misma información sobre los riesgos de las operaciones electrónicas ni de los mecanismos disponibles para evitarlos y, iv) este régimen de responsabilidad crea un incentivo para que los bancos implementen dichas medidas (Jiménez, 2025). En cuanto a la Protección de datos personales en el sector financiero, deben tenerse en cuenta también: la Ley 1273 de 2009 que tipifica los delitos informáticos en Colombia, la Ley 1266 de 2008 que regula el Habeas Data Financiero, el Decreto 2555 de 2010, establece obligaciones sobre protección de datos personales en el sistema de pagos de bajo valor, y la Circular Externa 029 de 2019 de la Superintendencia Financiera que establece lineamientos sobre seguridad de la información en el sector financiero, desarrollos jurisprudenciales de la Corte Suprema de Justicia y la Corte constitucional.

seguridad y a contener los efectos del incidente en su reputación[2].

En un régimen de Responsabilidad Demostrada, en el que el Responsable debe acreditar la adopción de medidas de seguridad "efectivas" y "adecuadas", la ocurrencia de una violación de seguridad tiende a operar, en la práctica, como un indicio de que dichas medidas no fueron suficientes. Dado que la condena y la sanción resultan automáticas a partir del incidente, con independencia de la diligencia ex ante del Responsable, la inversión en medidas de seguridad no garantiza la exclusión de responsabilidad *ex post*.

Esta estructura genera un problema de incentivos —*moral hazard*—: si el Responsable no puede anticipar con certeza si las medidas adoptadas serán consideradas razonables o efectivas por la autoridad o por un juez, la inversión en seguridad pierde capacidad de reducir el riesgo jurídico. En ese escenario, resulta racional que los Responsables orienten sus recursos hacia mecanismos de gestión del riesgo posterior —como seguros, notificación y defensa jurídica— en lugar de hacia la prevención, sin que ello implique necesariamente una mejora en la seguridad efectiva de los datos.

En efecto, la literatura económica ha mostrado que, cuando las empresas enfrentan costos crecientes de inversión en ciberseguridad pero con beneficios decrecientes —cada medida de seguridad adicional es más costosa que la anterior pero ninguna logra eliminar del todo el riesgo de un incidente de seguridad— y actúan de forma no cooperativa, tienden a sub-invertir en medidas preventivas (seguridad) y a sustituir estas medidas por mecanismos de transferencia del riesgo, como el ciberseguro, generando equilibrios ineficientes desde el punto de vista social (Boonen et al, 2025)[3].

El punto, más allá de si la responsabilidad es objetiva o subjetiva, es que en el contexto de la responsabilidad administrativa los ciberataques, bajo ciertas circunstancias que se verán más adelante, deberían ser considerados como eximentes de responsabilidad por tratarse de un hecho de un tercero que muchas veces es imprevisible e irresistible a pesar de haber implementado medidas de seguridad adecuadas.

3. Las obligaciones impuestas por el deber de seguridad

Uno de los deberes u obligaciones de los Responsables y Encargados consiste en preservar los datos seguros; es decir, evitar el acceso no autorizado a los datos para preservar así su integridad, confidencialidad y reserva. Determinar qué implica exactamente este deber y hasta dónde llega la responsabilidad de los Responsables y Encargados en caso de un ciberataque o de una violación o falla de las medidas de seguridad es fundamental para que los Responsables y Encargados puedan eximirse ante un juicio de responsabilidad y, sobre todo, para que al momento de implementar sus programas de *Principle Accountability* o de PRD sepan qué pruebas, documentación o programas de seguimiento son suficientes para demostrar que en efecto adoptaron medidas para cumplir con sus obligaciones.

El deber de seguridad está consagrado en el artículo 32 del GDPR, el cual establece que "el responsable del tratamiento y el encargado del tratamiento aplicarán medidas técnicas y organizacionales apropiadas para garantizar un nivel de seguridad adecuado al riesgo". Asimismo, este artículo establece que deben tenerse en cuenta varios aspectos frente a las medidas que deben implementar el Responsable y el Encargado como el estado de la técnica, los costes de aplicación o implementación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como la probabilidad y la gravedad del riesgo para los derechos y libertades de las personas.

Así el punto de referencia de "garantizar un nivel de seguridad adecuado al riesgo" implica que deben implementar medidas que sean conmensurables con el riesgo. Entonces, al evaluar las medidas adoptadas se debe identificar primero el riesgo y su potencialidad o probabilidad. Las medidas y controles deben estar basadas en una evaluación de riesgo (Koolen et al., 2024). Con este enfoque de regulación basado en la evaluación de riesgos se buscaba "cambiar la protección de datos de un simple cumplimiento de requisitos a una protección práctica, matizando las obligaciones de los Responsables del tratamiento de datos en función del riesgo involucrado" (Macenaite, 2017, p. 515). Este matiz se materializaría en dos aspectos: i) calibra las medidas que deben tomar

2 Sobre este punto, D. J. Solove hace un interesante análisis sobre la importancia de que las sanciones por la violación a las normas de protección de datos personales creen un verdadero incentivo la cumplimiento; esto porque las empresas saben que las ANPD no tienen muchos recursos y van a priorizar sancionar a aquellas empresas con incumplimientos más graves (Solove, 2026).

3 Por supuesto hay otros mecanismos jurídicos por los cuales el Responsable podría ser condenado a pagar o resarcir los daños causados por una violación a los códigos de seguridad o un ataque cibernético, como aquella derivada por la comercialización de productos defectuosos. En este campo una responsabilidad objetiva (*strict liability*) tiene importantes ventajas frente a un esquema de responsabilidad subjetiva (Negligence). Por un lado, sirve como incentivo para que las empresas que creen y distribuyen dispositivos con IoT implementen seguridad por diseño y por defecto. Por otro lado, aliviana la carga de la prueba de los consumidores, quienes no tienen los medios ni el conocimiento para demostrar que la falla en la seguridad se debió a una falta de diligencia del Responsable (Gardner, 2024).

los Responsables y Encargados de acuerdo con el riesgo y, ii) tales medidas deben responder a los riesgos reales para proteger los derechos de los Titulares (Quelle, 2017).

Ahora bien, el artículo 32 del GDPR plantea algunas medidas de seguridad que pueden implementarse (seudonimización, por ejemplo) y señala además algunos criterios que deben tenerse en cuenta al momento de escoger las medidas como el costo de implementación, lo que conduce a la aplicación del Principio de Proporcionalidad entre los derechos de los Titulares y criterios económicos del Responsable y el Encargado (Selzer, 2021). Las medidas de seguridad que adopte el Responsable deben ser tanto organizacionales como tecnológicas, y deben responder también a la obligación de implementar mecanismos de seguridad por defecto y por diseño (Mantelero et al., 2020).

Esta configuración del deber de seguridad responde a que, en materia de ciberseguridad y tecnología, determinar de forma estricta y detallada las medidas de seguridad rápidamente las haría vetustas y crearía una necesidad de constante actualización normativa o legislativa. Mientas que este enfoque basado en un análisis de riesgo mantiene la normatividad activa y actualizada a medida que cambian los riesgos, además, de implementar la neutralidad tecnológica.

Sin embargo, el enfoque basado en el análisis de riesgo por los Responsables también dificulta precisar el alcance de sus obligaciones y responsabilidades. Por ejemplo, si se cumple con el deber de seguridad solo con la implementación de las medidas de seguridad conforme al riesgo identificado —así las medidas no sean completamente efectivas— o qué sucede si el Responsable hace una evaluación de riesgo, pero las medidas no abordan correctamente los riesgos identificados o, incluso, si la evaluación del riesgo es adecuada pero el costo de implementación de las medidas es muy elevado y el Responsable decide implementar unas medidas de menor efectividad, o incumple la obligación de seguridad un Responsable que pese a haber adoptado medidas acordes con los riesgos identificados y con los estándares de la industria sufre un ciberataque —un ataque imprevisible e irresistible— por parte de un tercero.

Quelle (2017) señala que este enfoque basado en el riesgo, que se fundamenta en los artículos 24, 25 y 35 del GDPR, tiene un doble impacto respecto de las obligaciones del Responsable. Por un lado, implican una calibración de las medidas que debe tomar el Responsable para proteger los derechos y libertades del Titular, basado en una evaluación del riesgo y adopción de medidas acordes para proteger esos derechos. En otras palabras, las medidas técnicas y organizacionales deben ser escalables conforme al riesgo, pero también suficientes para proteger los derechos de los Titulares (. Sin embargo, la autora también señala que este enfoque tiene limitaciones en su ejecución por parte de las autoridades porque no existe en el GDPR una obligación autónoma e independiente sobre los Responsables para que mitiguen los riesgos frente a los derechos de los Titulares, sino que la obligación consiste en tener en cuenta el riesgo cuando se implementen otras obligaciones de la GDPR.

Cabe señalar que la GDPR no es la única normativa que aborda e impone obligaciones en materia de ciberseguridad en Europa, otras disposiciones como la Directiva sobre servicios de pago y el reglamento de identificación electrónica, entre otras, también abordan este tema, pero la GDPR es la más genérica y amplia en espectro (Mantelero et al., 2020).

En Colombia, el artículo 4 de la Ley 1580 de 2012, establece que uno de los principios para el tratamiento de los datos personales es el de seguridad y que tanto Responsable como Encargado deben tratar los datos con **"**las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento." Adicionalmente, el artículo 17, literal d), de la misma ley señala que es deber del Responsable "conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento." Por su parte el apartado i) de este artículo establece como otro deber del Responsable es el "exigir al Encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular".

La redacción de estos deberes de los Responsables del tratamiento podría entenderse o interpretarse como una obligación de resultado objetiva, que no permite ningún tipo de eximente de responsabilidad frente a una eventual violación de las medidas de seguridad porque de haber algún incidente o violación no se habrían adoptado las "condiciones de seguridad necesarias para impedir" la adulteración, pérdida, consulta, etc. de los datos personales. En otras palabras, la forma en que está redactado el deber de seguridad de los Responsables implica que, de haber alguna adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, sin importar el origen de la falla de seguridad, no se cumplió con tal deber porque las medidas adoptadas no lograron impedir que ocurriera el incidente y que las medidas implementadas no fueron las que se necesitaban para preservar la seguridad del dato.

La ANDP en Colombia emitió la Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales. En esta, se señala que el principio y el deber de seguridad tienen un "criterio eminentemente preventivo" que implica que Responsables y Encargados deben adoptar las medidas necesarias "para evitar posibles afectaciones a la seguridad de los datos". Si las medidas de seguridad fallan se deben adoptar otras para mitigar los daños que ello pueda causar a los derechos de los Titulares, como informar del incidente a la autoridad y a los Titulares (Superintendencia de Industria y Comercio, 2020). Esto podría entenderse como que el deber de seguridad no es objetivo ni absoluto, de forma que debería bastar para eximirse de responsabilidad con demostrar que se adoptaron medidas de seguridad acordes con el tipo de dato tratado parar prevenir o mitigar el riesgo de ciberataques y, en caso de un incidente, informar a la ANPD y a los Titulares.

Respalda lo anterior que la seguridad de los datos no es un fin en sí mismo si no que es un medio para alcanzar otros principios y hacer efectivos otros derechos de los Titulares (Oficina del Alto Comisionado de las Naciones Unidas., 2022). En efecto, con la seguridad lo que se busca es que; por ejemplo, no se robe la identidad del Titular. También, que no se divulguen datos sensibles que puedan generar discriminación en contra del Titular o simplemente que no se conozca información que pertenece a la esfera íntima del Titular del dato.

En ese sentido, la falla de una medida de seguridad no debería generar automáticamente la responsabilidad administrativa y/o civil del Responsable o Encargado, sino que si se aplica también el PRD, debería analizarse primero la evaluación de riesgo efectuada para determinar si el riesgo era previsible y resistible y si las medidas implementadas eran razonables, así como evaluar efectivamente el daño actual o potencial sobre los derechos de los Titulares. Al respecto del último punto, debería tenerse en cuenta la evaluación de los riesgos e impacto del incidente de seguridad que recomienda la ANDP que debe hacerse luego de la ocurrencia de un incidente (Superintendencia de Industria y Comercio, 2020). En dicha evaluación se determinará el impacto de incidente en los derechos de los Titulares.

Teniendo en cuenta que los incidentes de seguridad pueden originarse en hechos de terceros que de forma maliciosa y con fines lucrativos vulneran las medidas de seguridad que adoptan los Responsables ya sea a través de *phishing*, malvare, etc. (Antoni Gobeo, 2022) y que muchas veces estos ciberataques son imprevisibles e irresistibles (Tacha, 2024) deberían actuar como eximentes de responsabilidad incluso administrativa del Responsable.

En efecto, la previsibilidad de los ataques cibernéticos es crucial para determinar si se cumplió o no con el deber de seguridad porque se ha aceptado que es imposible evitar por completo o al 100 % esos ataques. De hecho, el riesgo residual es aquel que permanece incluso después de haber adoptado medidas de seguridad y debido a que siempre va a estar allí, lo que se recomienda para mitigarlo es hacer seguimiento constante y adoptar controles para que sea un riesgo "aceptable" (Sánchez García, 2023). Adicionalmente, porque es el Responsable no causa el daño o la violación de la seguridad, sino que es un tercero el que se aprovecha de una brecha para causar estos ciberataques que dañan o afectan los derechos del Titular (Tschider, 2023).

Considerando la imposibilidad de evitar por completo los ataques cibernéticos, Tschider (2023) propone una evaluación en dos pasos de la razonabilidad de las medidas de seguridad implementadas. Primero, un análisis estático, para determinar si las medidas implementadas cumplen con estándares de seguridad reconocidos y es acorde con las prácticas industriales y los marcos técnicos existentes. Segundo, una evaluación dinámica que considera las circunstancias concretas en las que se presentó el ataque, los riesgos previsibles, el tipo de datos tratados y se analiza si las decisiones tomadas frente al riesgo fueron razonables. De esta forma, la materialización del ataque no prueba por sí mismo el incumplimiento en las obligaciones del Responsable, sino que se evalúa la razonabilidad de las decisiones tomadas *ex ante*.

4. Aplicación del PRD en casos de ciberataques en LATAM

El PRD ha sido adoptado por varias regulaciones, particularmente la europea que luego influyó en los países de Latinoamérica que buscaban tener un nivel adecuado de protección que permitiera el flujo de datos hacia estos países, aunque no puede decirse que se trate de regulaciones uniformes (Arenas, 2022). En el presente apartado, se analizará con casos concretos cómo las ANPD han aplicado el PRD al evaluar casos de violaciones o falta de medidas de seguridad de los datos personales. En particular, se estudiarán casos de Colombia, Brasil, Perú y México, para luego hacer algunas anotaciones sobre las posturas adoptadas en estos países y la posibilidad de considerar los ciberataques como eventos de fuerza mayor eximente de responsabilidad.

4.1. Colombia

En Colombia, el PRD se implementó mediante el artículo 26 del Decreto 1377 de 2013, por el cual se reglamentó la Ley 1581 de 2012, la Ley Estatutaria de Protección de Datos Personales en el país. Este artículo señala que los Responsables deben ser capaces de "demostrar a petición de la

Superintendencia de Industria y Comercio (SIC, en adelante), que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas" en la Ley. En seguida, la norma agrega que esas medidas deben ser proporcionales a la naturaleza jurídica del Responsable, su tamaño empresarial, la naturaleza de los datos que trata, el tipo de tratamiento que realiza y los riesgos potenciales que se deriven del tratamiento a los derechos de los Titulares.

Como se mencionó antes, la Ley 1581 de 2012 establece en el artículo 4 el Principio de Seguridad en el Tratamiento de los Datos y que los Responsables deben adoptar las medidas técnicas, humanas y administrativas que sean necesarias para preservar la seguridad y evitar su adulteración, pérdida, consulta, uso o acceso no autorizado. Cabe señalar que esta misma Ley establece que la SIC es la ANPD del país.

La SIC emitió una Guía para la implementación del PRD en la cual se explica que, conforme al Decreto 1377 de 2016, el PRD es una obligación en cabeza de los Responsables, quienes a petición de la SIC deben ser capaces de demostrar que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones que les impone la ley estatutaria. Posteriormente, se añade en esta guía que las medidas se deben adoptar "teniendo en cuenta diversos factores que son propios de cada organización —como— su tamaño y naturaleza jurídica, la naturaleza de los datos tratados, el tipo de tratamiento [...] y los riesgos que implique para los Titulares la recolección y posterior uso o circulación de los datos" (Superintendencia de Industria y Comercio, p. 6). La Guía también destaca como una ventaja de la implementación del PRD que, si se verifica la existencia de medidas y políticas para el adecuado tratamiento de los datos "será tenida en cuenta al momento de evaluar la imposición de sanciones", como lo señala el Decreto 1377 de 2013.

Con relación a los incidentes de seguridad, la guía indica que debido a que la regulación colombiana no define ni distingue diferentes tipos de incidentes de seguridad, "independientemente de su impacto, deben reportarse a esta autoridad todos los incidentes ocurridos." Además, los Responsables, ante la ocurrencia de incidentes de seguridad y en implementación del PRD deberían, no solo reportar el incidente a la autoridad sino i) informar al Titular del dato, y ii) "proporcionar herramientas a dichos Titulares afectados para minimizar el daño potencial o causado" (Superintendencia de Industria y Comercio, p. 20) .

También, existe en Colombia una Guía para la aplicación del principio de seguridad, que parte por señalar que el principio de seguridad es preventivo y que es deber de Responsables y Encargados adoptar las medidas necesarias para evitar afectaciones a la seguridad de los datos (Superintendencia de Industria y Comercio, 2020). También se aclara en la Guía que no se indican medidas de seguridad concretas para la gestión de incidentes porque estas dependen de cada caso concreto, y se explica con un enfoque práctico cómo se debe actuar en caso de un incidente (Superintendencia de Industria y Comercio, 2020).

En línea con el carácter preventivo del deber de seguridad, la guía señala que las medidas de seguridad "deben ser apropiadas considerando varios factores como: i) los niveles de riesgo del Tratamiento para los derechos y libertades de los Titulares de los datos; ii) la naturaleza de los datos; iii) las posibles consecuencias que se derivarían de una vulneración para los Titulares, y la magnitud del daño que se puede causar a ellos, al Responsable y a la sociedad en general; iv) el número de Titulares de los datos y la cantidad de información; v) el tamaño de la organización; vi) los recursos disponibles, vii) el estado de la técnica, y viii) el alcance, contexto y finalidades del Tratamiento de la información" (Superintendencia de Industria y Comercio, 2020, p. 12).

De lo anterior se tiene que el PRD implica tener las pruebas y respaldo de la adopción de medidas de seguridad que según el Responsable sean apropiadas, teniendo en cuenta factores como el nivel de riesgo y la magnitud de la afectación a los derechos de los Titulares, pero también el tamaño de la organización y los recursos disponibles. Entonces, se reitera, la mera ocurrencia de un incidente de seguridad no debería implicar *per se* la responsabilidad administrativa del Responsable, sino que debería analizarse primero la evaluación de riesgo efectuada para determinar si el riesgo era previsible y resistible y si las medidas implementadas eran razonables.

Ahora, pasando a los casos concretos, en dos resoluciones del 28 de julio de 2023 la SIC impuso órdenes a dos empresas que informaron haber sufrido incidentes de seguridad. Aunque las resoluciones no detallan en qué consistieron los incidentes, la SIC debía analizar si se configuraba una violación al literal d) del artículo 17 de la Ley 1581 que consagra el deber de conservar la información bajo condiciones de seguridad. Para ello primero la SIC señala que

> *para que se pueda extraer un juicio de responsabilidad como consecuencia de la infracción de esta obligación debe demostrarse que la información personal de los Titulares no se conservó bajo las condiciones de seguridad necesarias y puedo ser objeto de adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, rompiendo con los principios de circulación restringida y seguridad*

> *de la información* (Resolución 43407 de 2023, p. 2; Resolución 43249 de 2023, p. 2).

Luego de describir el principio de acceso y circulación restringida y el de seguridad, la SIC señala en su análisis que:

> *con fundamento en el incidente de seguridad reportado [por cada sociedad] y las medidas adoptadas para la gestión del incidente, esta Dirección considera necesario entrar a analizar las medidas y controles de seguridad con los que cuenta la sociedad [...], con el fin de determinar si las mismas son apropiadas y efectivas, garantizando los estándares de protección de información personal, así como proporcionales a la naturaleza jurídica y tamaño de la investigada, la naturaleza de los datos personales objeto del Tratamiento, tipo de Tratamiento, y los posibles riesgos que el Tratamiento podría causar sobre los derechos de los Titulares, en cumplimiento del Principio de Responsabilidad Demostrada recopilado por el artículo 2.2.2.25.6.1. del Decreto Único Reglamentario 1074 de 2015, y si es necesario establecer medidas de seguridad adicionales a las medidas con las que actualmente cuenta la investigada, para este propósito* (Resolución 43407, 2023, p. 3; Resolución 43249, 2023, p. 3).

De lo anterior pareciera que la SIC se adentraría en un análisis concreto respecto de las medidas de seguridad implementadas por cada una de las sociedades que reportaron los incidentes, que analizaría si las mismas fueron acordes con el tipo de datos personales tratados y el nivel de riesgo que el tratamiento implica para los Titulares, así como el riesgo de sus derechos en caso de acceso o uso no autorizado. Además, también se da a entender que la SIC analizaría las pruebas que cada sociedad aportó para demostrar que en efecto sus medidas de seguridad son acordes a estos parámetros. Sin embargo, la SIC simplemente señala que "no ha emitido un listado taxativo de las medidas de seguridad que deben implementar los Responsables y Encargados del Tratamiento de datos" (Resolución 43407 de 2023, p. 3; Resolución 43249 de 2023, p. 3). Además, agrega que los parámetros de las medidas de seguridad apropiadas y efectivas están en el Decreto 1074 de 2016 al establecer el PRD y la implementación de políticas internas efectivas.

Finalmente, en estas dos resoluciones la SIC señaló que:

> *si bien la sociedad puede contar con unos lineamientos mínimos para implementar las medidas de seguridad que considerara aptas y suficientes con el fin de garantizar la protección de los datos personales […], se hace necesario que la sociedad refuerce las medidas implementadas y realice constante seguimiento y mejoras a las buenas prácticas de las mismas a que no han sido suficientes para evitar un incidente* (Resolución 43407 de 2023, pág. 4; Resolución 43249 de 2023, pág. 4).

Nótese que la SIC no señala cuales fueron los incidentes de seguridad sufridos por las sociedades, tampoco analiza si las medidas de seguridad eran apropiadas o suficientes confirme a los parámetros señalados por ella misma —tamaño de la sociedad, tipo de datos, y riesgo para los Titulares, etc.— sino que el final señala que tales medidas "no han sido suficientes para evitar un incidente". De forma que en realidad pareciera que no importa que la empresa sea juiciosa en la implementación de medidas humanas, administrativas y técnicas dirigidas a prevenir estos ataques, sino que, si es víctima de un ciberataque, como tales medidas no lo evitaron, habrá incumplido con su obligación y podrá ser sancionada.

Esto refuerza el *moral hazard* abordado anteriormente. Si no importa qué medidas de seguridad implemente la empresa, siempre habrá un riesgo residual que, de materializarse en un incidente, puede llevarlo a grandes sanciones, sin hablar de la afectación a su reputación. Por ello, resulta más racional que la empresa opte por gastar en seguros que trasladen a un tercero el potencial costo de la sanción e incluso de la reparación a los Titulares.

Cabe señalar que el razonamiento de la SIC se replica con texto prácticamente idéntico en la Resolución 40704 de 2021, en las número 70773, 70784, 75732 y 75741 de 2022, así como las resoluciones 43249, 43325 de 2023, por lo que se evidencia que esta ha sido una postura reiterada de la SIC.

Sin perjuicio de lo anterior, se han presentado algunos casos en los que el análisis de la ANDP de Colombia ha sido un poco más profundo. De una parte, en caso de UBER en 2019 en el que, si bien la decisión de la SIC estuvo fundamentada principalmente en decisiones de autoridades foráneas, se estudió y abordaron las medidas de seguridad concretas que había tomado el Responsable en el caso concreto. De otra parte, el caso de ScotiaBank Colpatria S.A. en 2025, en el que un empleado del banco remitió a su correo personal archivos cifrados con datos personales de los clientes del banco.

Analizando primero el caso de UBER, este tuvo basta relevancia internacional, corresponde al incidente sufrido por UBER en el 2017 y que llevó a la imposición de ordenes por parte de la SIC mediante la Resolución 21478 de 2019. A finales de 2016, dos personas ingresaron fraudulentamente a los nombres y números de licencia de 600.000 usuarios de UBER —de los cuales aproximadamente 267.000 eran colombianos— alojados en una nube de AWS. La ocurrencia del incidente fue divulgada públicamente un año después por el CEO de la compañía. El incidente se debió a que todos los

ingenieros de UBER usaban una única clave para acceder a la información almacenada en la nube y la clave fue publicada en internet por uno de los ingenieros de la empresa.

Siguiendo las investigaciones adelantadas por ANPD de otros países como Estados Unidos, Reino Unido, Francia, entre otras, la SIC impuso a UBER una serie de ordenes dirigidas a que se mejoraran las medidas de seguridad para prevenir ataques. Esto como quiera que las implementadas no fueron las "suficientes y necesarias, para impedir que terceras partes en este caso: atacantes externos, accedieran sin autorización al sistema de almacenamiento Amazon Web Services AWS's y descargaran [datos personales, incluso sensibles]" (Resolución 21478 de 2019, p. 32). La SIC tuvo en cuenta que UBER no implementó medidas de autenticación multifactor, que no informó oportunamente a los Titulares de la ocurrencia del incidente, no mejoró sus sistemas de seguridad pese a que había sufrido ataques similares en el pasado.

Ahora, en el caso de ScotiaBank Colpatria S.A., la SIC impuso una sanción por más de setecientos millones de pesos (aprox. USD 200.000) por violación a medidas de seguridad. La entidad financiera fue informada —por la Asociación para la Investigación, Información y Control de los Sistemas de Tarjetas de Crédito y Débito INCOCRÉDITO— de haber encontrado una base de datos de sus clientes en un centro de atención telefónica asociado a varias reclamaciones de fraude con tarjetas de crédito.

Por ello, ScotiaBank inició una investigación interna por la que concluyó que un funcionario activo había extraído información de clientes del banco valiéndose de excepciones al sistema de *Data Loss Prevention* (DLP) de las que gozaba en razón a su cargo. Aunque no se estableció si él vendió esa información a terceros, sí que durante cuatro estuvo extrayendo información que no podía extraer directamente, sino que le debía ser suministrada por otros funcionarios del banco (Resolución 70035 de 2025).

El empleado del banco contaba con una excepción al DLP debido a que una de sus funciones era suministrar información sobre mora de los clientes del banco a las centrales de riesgo y remitir reportes a entes reguladores para lo que requería acceso a los datos personales y envío a cuentas externas de terceros ajenos al banco (Resolución 70035 de 2025).

En las consideraciones de la SIC respecto de si esta situación constituye una violación al principio de seguridad y al deber de implementar las medidas de seguridad necesarias para evitar el acceso y uso no autorizado a los datos personales, se resalta que el Banco no realizó un control sobre los destinatarios con los cuales el empleado compartía información de los Titulares, pues se evidenció que entre 2021 y 2022 el empleado envió 297 correos con datos personales en archivos ZIP a un correo personal sin que el banco tuviera noticia de ello (Resolución 70035 de 2025). Adicionalmente, que el sistema de DLP implementado contaba con controles y alarmas que se activaban únicamente frente al tipo y cantidad de información enviada a terceros, pero no según el destinatario de la información —cuentas comerciales como Gmail o Hotmail—. Las medidas de seguridad tampoco tuvieron en cuenta ni generaron alarma que en un solo mes el empleado se enviara 30 correos a su cuenta personal. Sobre este punto vale la pena resaltar lo señalado por la SIC respecto de las medidas de seguridad implementadas por el banco:

> *[...] situación que no fue identificada por SCOTIABANK COLPATRIA S.A., porque no implementó las medidas de seguridad necesarias para los pocos usuarios con privilegios de envío de información, pues si bien la sociedad tomó medidas para restringir a la mayoría de sus empleados el uso de estas prerrogativas, era precisamente para poder controlar la información compartida, sin embargo, los controles no fueron los necesarios y suficientes para el tipo y la cantidad de información tratada por el banco* (Resolución 70035 de 2025, p. 38).

Esta cita muestra mayor análisis a cerca de la relación entre los motivos del incidente de seguridad y las medias implementadas por el Responsable, señalando que si bien existieron algunas que impedían envío de datos personales por parte de un gran número de empleados del Banco, frente aquellos con excepciones no existían verdaderos controles de seguridad, los cuales sí fueron implementados con posterioridad al incidente. Esto es, que para envío de información a correos con cuentas comerciales, la información estaría en cuarentena y sólo luego de ser autorizado sería posible el envío (Resolución 70035 de 2025).

Por ello, la SIC consideró que el incidente no podía considerarse únicamente como un abuso o extralimitación en las funciones del empleado, sino una verdadera falla en las medidas de seguridad implementadas. Cabe señalar que el empleado que incurrió en estas conductas también fue sancionado e incluso se promovieron acciones penales en su contra.

4.2. Brasil

En Brasil, el PRD está consagrado en el artículo 6, inciso X, de la Ley 13.709 de 2018, Ley General de Protección de Datos Personales. Allí se establece que el tratamiento de los datos personales debe seguir una serie de principios dentro de los que se encuentra la responsabilidad y la transparencia que consisten en la "*demostración por parte del agente de la adopción de medidas eficaces capaces de probar*

la observancia y el cumplimiento de las normas de protección de datos personales e incluida la eficacia de estas medidas".

Cabe señalar también el Reglamento sobre comunicación de incidentes de seguridad (Resolução CD/ANPD N.º 15/2024, 2024). Este reglamento define los incidentes de seguridad como "cualquier evento adverso confirmado, relacionado con la violación de las propiedades de confidencialidad, integridad, disponibilidad y autenticidad de la seguridad de los datos personales". En sus artículos 4 y 5 señala que se deben notificar a la ANPD brasilera aquellos incidentes de seguridad que puedan acarrear un riesgo o daño relevante a los Titulares del dato y que un riesgo o daño es relevante cuando cumple alguno de los siguientes criterios: "i) datos personales sensibles; ii) datos de niños, adolescentes o personas mayores; iii) datos financieros; iv) datos de autenticación en sistemas; v) datos protegidos por secreto legal, judicial o profesional; o vi) datos tratados a gran escala".

Adicionalmente, el Reglamento sobre notificación de incidentes establece que la ANPD podrá iniciar procesos administrativos dirigidos a investigar el incidente, ordenar medidas correctivas, realizar auditorías o inspecciones a los Responsables.

La ANPD de Brasil ha aplicado el PRD frente a incidentes de seguridad presentados en entidades públicas. En uno de estos casos, la Secretaría de Educación del Distrito Federal implementó un formulario en Google Forms para la inscripción en el Programa de Educación Infantil Temprana para evitar inscripciones duplicadas, reducir los tiempos de espera y mejorar la accesibilidad al programa. Sin embargo, las respuestas al formulario podían ser accedidas por terceros dada una programación preestablecida por Google Forms aunque la entidad no hubiera compartido el enlace. Como consecuencia, era posible acceder a datos de 3.030 personas, principalmente menores de edad.

La Coordinación General de Supervisión (unidad técnica del a ANPD de Brasil) fue la que informó del incidente seguridad a la Secretaría de Educación del Distrito Federal y solicitó una evaluación de impacto sobre el incidente de seguridad y sobre la adopción de las medidas técnicas y administrativas necesarias para garantizar la seguridad de la base de datos afectada.

La ANPD debía decidir si esta situación constituyó una violación al artículo 49 de la Ley 13.709 de 2018, la Ley General de Protección de Datos Personales referente al uso de uso de sistemas que cumplan con los requisitos de seguridad, las mejores prácticas y los estándares de gobernanza, y los principios de la Ley General de Protección de Datos Personales.

La ANDP señaló que "*el incidente de seguridad se debió a una configuración realizada por un usuario en la herramienta Formularios de Google, que permitió a personas no autorizadas acceder a las respuestas enviadas*". De forma que en realidad no se trataba de un incidente de seguridad sino de una falla en la adopción de medidas de seguridad administrativas, conforme lo exige el artículo 6 de la mencionada ley.

Frente a este punto, la ANPD aceptó la explicación de la Secretaría de Educación del Distrito Federal de que no fue posible capacitar en el uso de las herramientas como Google Forms porque estas debieron emplearse aceleradamente con motivo del COVID-19, es decir, aceptó que en este caso no se hubieran adoptado medidas administrativas para resguardar la seguridad de los datos (Autoridade Nacional de Proteção de Dados, 2024, p. 29).

En otro caso, relativo al Instituto Nacional de la Seguridad Social (INSS), se evidenció que los datos de varias personas beneficiarias del sistema de salud fueron consultados de forma masiva e irregular, aunque empleando usuarios y claves de acceso habilitadas, la discusión se centró en el deber de notificar a los Titulares de la ocurrencia del incidente para que pudieran adoptar las medidas que estimaran pertinentes para proteger su información.

El INSS se oponía a tal comunicación alegando, primero, que era técnicamente imposible identificar a los Titulares de datos afectados, segundo, que una comunicación masiva a todas las personas inscritas en el SISBEN generaría desconfianza y afectaría el interés general; y, tercero, que la información relativa a la falla de seguridad tenía el carácter de información reservada por su relación con la seguridad nacional. La ANPD de Brasil descartó estos argumentos.

Frente al segundo argumento, se señaló que el deber de información de los incidentes busca proteger un derecho fundamental porque el acceso no autorizado a los datos puede afectar gravemente a los Titulares, más si se considera que se tuvo acceso a datos personales sensibles como información médica e información de pagos. De forma que los Titulares del dato tienen una expectativa legítima de ser informados en caso de que por un incidente sus datos estén en peligro. Asimismo, enfatizó la autoridad que no cumplir con esta obligación acentúa la asimetría de información que existe entre el Responsable y el Titular del dato (Autoridade Nacional de Proteção de Dados, 2024).

En otros casos, ahora referentes a acciones civiles el Tribunal Superior de Justicia (TSJ) se pronunció recientemente acerca de la obligación del Responsable de reparar al Titular en casos de

ciberataques[4]. Sobre este punto, se debe notar que la Ley de Protección de Datos Personales (LGPD) brasilera establece que los Responsables están obligados a reparar los daños patrimoniales, morales, individuales o colectivos que generen por la violación de la ley y establece unos parámetros para asegurar la efectiva reparación del Titular.

Uno de esos instrumentos es la intervención de juez en los procesos civiles, donde podrá invertir la carga de la prueba a favor del Titular cuando no cuente con recursos técnicos, organizativos o informáticos para producir la prueba y le resulte excesivamente oneroso (Artículo 42 § 2, LGPD). Adicionalmente, la LGPD establece que los Responsables pueden eximirse de sanciones cuando prueben que, entre otras, el daño es consecuencia de la culpa exclusiva del Titular o de un tercero (artículo 43, ítem III, LGPD).

En el caso de *Eletropaulo Metropolitana Eletricidade de Sao Paulo S.A.*, una usuaria alegaba indemnización de daños morales por la violación a su privacidad derivada de una divulgación no autorizada de datos personales gestionados por la empresa mencionada. Aunque la condena de daños morales fue descartada, se ordenó informar al Titular con quién se habrían compartido los datos, entregar copia completa de los mismos y remitir el caso a la ANPD.

La empresa apeló alegando que la divulgación se debía exclusivamente a un ataque de un tercero y que había adoptado las medidas de seguridad pertinentes. En consecuencia, el TSJ debía decidir si el ciberataque eximiese de responsabilidad al Responsable —*Eletropaulo Metropolitana Eletricidade de Sao Paulo S.A.*—. El TSJ consideró que el Responsable tiene que adoptar medidas de seguridad de acuerdo con las técnicas disponibles al momento del tratamiento y que este es un nivel de seguridad que el Titular tiene derecho a esperar —expectativa legítima de seguridad—. Debido a que el Responsable no demostró que el ciberataque fuera la única causa de la divulgación ni que sus medidas de seguridad fueran suficientes y eficaces, se concluyó que un ciberataque no elimina automáticamente su responsabilidad (AREsp 2.170.495/SP, 2025).

En otro caso, la usuaria de una entidad financiera solicitó por correo electrónico información sobre la deuda asumida con la finalidad de pagarla y liquidarla, días después fue contactada vía WhatsApp con información sobre el crédito, el monto adeudado, las cuotas pagadas etc. La usuaria procedió al pago sin saber que se trataba de una estafa. Posteriormente, el banco reclamaba el pago de la deuda y la usuaria se oponía alegando que ya lo había pagado y que el fraude era atribuible a la entidad financiera.

El TSJ respaldó la postura de la usuaria considerando que los estafadores tuvieron acceso a datos personales que sólo debían ser de conocimiento del banco. Más allá de los datos de contacto, la información sobre los servicios contratados, el monto pagado y la deuda, era información que debía preservar en confidencialidad el Banco lo que evidenciaba una falla en el servicio que le era atribuible. También destaca el TSJ un estándar al nivel de seguridad que debería esperarse del banco con fundamento en la LGPD, así:

> En cuanto al artículo 44 de la LGPD, la doctrina enseña que «la norma destaca, al igual que ocurre en relación con la responsabilidad del proveedor en la CDC, la cuestión relativa a los riesgos de desarrollo, ya que limita el alcance del deber de seguridad a lo esperado debido a las técnicas de tratamiento de datos disponibles en el momento de su realización" y, considerando "la previsibilidad de una actualización y un avance técnico en las actividades vinculadas a la tecnología de la información, más rápido que en otras actividades económicas." (Recurso Especial N.º 2.077.278 - SP, p. 15)

En una decisión similar, el TSJ señaló que los Titulares de los datos tienen una expectativa legítima de protección y que el tratamiento de los datos se considera irregular cuando no proporciona las medidas de seguridad que el Titular podía esperar teniendo en cuenta las circunstancias relevantes, incluidas las técnicas de tratamiento de datos personales disponibles al momento en que el mismo se realizó. En ese sentido, aunque no se señaló exactamente en qué consistió el incidente de seguridad, sí se indicó que al no haberse probado que "la filtración de los datos del demandado se produjo exclusivamente debido al incidente de seguridad, no es posible aplicar a favor del recurrente la exclusión de responsabilidad del art. 43, III, de la LGPD" (REsp 2.147.374/SP, STJ, 3ª Turma, 2024).

La postura del TSJ ha incluso señalado que el deber de seguridad es mayor cuando se tratan datos sensibles, por ejemplo, aquellos relacionados con aspectos familiares, personales, financieros y de salud de las personas cuando contratan seguros. En Efecto, el TSJ ha señalado que la filtración de estos datos expone al Titular a diversos riesgos en varios aspectos de su vida y que por ello "la provisión indebida de datos personales por parte de bases de datos a terceros constituye un presunto daño moral (*in re ipsa*) para el Titular de los datos registrado, especialmente dada la profunda sensación de

4 Existen otros pronunciamientos del TSJ referentes a la obligación de probar daño para que haya lugar a indemnización (AREsp N.º 2.130.619-SP) Sin embargo, no se aborda acá porque no se analizó en profundidad el deber de seguridad ni el PRD.

inseguridad que experimenta" (REsp 2.121.904/SP, STJ, 3ª Turma). Aunque en otros casos ha sostenido que el daño moral debe ser demostrado por el Titular (AREsp N.º 2.130.619-SP, 2023).

4.3. Perú

La Ley peruana de Datos personales, Ley N.º 29733 de 2011, establece en su artículo 9 el Principio de Seguridad, en virtud del cual el Titular del banco de datos (equiparable al Responsable) debe adoptar "*las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales.*" Y agrega que estas medidas deben ser acordes con el tratamiento y con la categoría de datos de que se trate.

La doctrina peruana ha señalado que el principio de seguridad, aunque es un mandato de optimización que no impone obligaciones específicas, sí tiene al menos tres objetivos que imponen obligaciones materiales al Titular del banco de datos —Responsable—: i) una evaluación continua de los bancos de datos y los riesgos que conlleva su tratamiento para identificar las medidas técnicas adecuadas; ii) informar la importancia de la seguridad de los datos; y ii) "*exigir un nivel de seguridad equilibrado entre los riesgos, las técnicas de seguridad y el costo de las medias"* (Alvarado, 2016).

Cabe señalar que Perú cuenta con normas técnicas que establecen parámetros para la seguridad de la información y que se toman como referentes para evaluar si las medidas de seguridad implementadas por el Titular del banco de datos —Responsable— son suficientes (DGPDP, 2013). Así como un reglamento a la Ley N.º 29733 de 2011, el Decreto Supremo N.º 16 de 2024 por el cual se establecen nuevas obligaciones a los Responsables, nuevos derechos para los Titulares —como el de portabilidad de los datos— y se establecen parámetros más claros en casos de incidentes de seguridad (Ministerio de Justicia y Derechos Humanos, Perú, 2024).

El principio de responsabilidad proactiva, como se denomina en Perú al PRD, no se encontraba inicialmente en la Ley N.º 29733 de 2011. Sin embargo, la doctrina del país señalaba la posibilidad de tenerlo incorporado al ordenamiento argumentando que los principios de la Ley en mención son meramente enunciativos y, considerando el Reglamento Europeo N.º 2016/679, la normativa peruana más que señalar acciones específicas en cabeza del Responsable establece una obligación final de proteger la privacidad y de "prevención ante cualquier amenaza existente o potencial" (Vásquez, 2022).

El principio de responsabilidad proactiva fue implementado expresamente en el artículo VII.2 del Decreto Supremo N.º 16 de 2024. Allí se indica que en el tratamiento de los datos se deben aplicar las medidas legales, técnicas y organizativas para garantizar el cumplimiento de la ley y que el Titular del banco de datos o quien sea Responsable "debe ser capaz de demostrar tal cumplimiento". Asimismo, este Decreto Supremo establece que este principio implica que se realice una evaluación de impacto o riesgos que pueda generar el tratamiento de los datos.

Ahora, pasando a casos concretos, a la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos de Perú se le consultó acerca del alcance de la obligación de seguridad del artículo 9 en caso de ciberataque; en concreto, si un ciberataque que diera lugar a la difusión no autorizada de datos personales podría ser considerado como una causa de fuerza mayor. A lo que se contestó que:

> En cuanto a la pregunta si podría ser considerado un ciberataque como una causa de fuerza mayor; cabe precisar que el Reglamento de la LPDP regula el cumplimiento de las obligaciones referidas a las medidas de seguridad, específicamente en los artículos 39º a 46º. Además, del cumplimiento del principio de seguridad. En ese sentido, la revelación y/o difusión de información de carácter personal sin consentimiento contraviene la LPDP y su Reglamento.
>
> Finalmente, en cuanto a la interrogante si se pudiese exonerar o eximir de sanción al Titular del banco de datos personales en razón de un ciberataque, cabe indicar que un acceso no autorizado que afecte la seguridad de los datos personales, incumple las medidas de seguridad requeridas por la LPDP y su reglamento para el tratamiento de datos personales hecho que podría acarrear responsabilidad administrativa (Ministerio de Justicia y Derechos Humanos, 2018).

Esta respuesta permite entrever la postura de la autoridad sobre potenciales incidentes de seguridad. En ella no se menciona la posibilidad si quiera de que un incidente o ataque a las medidas de seguridad implementadas pueda ser considerado como eximente de responsabilidad; si no que esto se considera un incumplimiento a las obligaciones del Responsable, lo que acarrearía sanciones administrativas.

El Banco de Crédito de Perú (BCP), en julio de 2018, sufrió un incidente de seguridad consistente en la instalación de un software malicioso que permitió a terceros no autorizados la consulta de información bancaria de 34.242 personas. Los datos comprometidos correspondían a nombre, dirección, correo electrónico, número de cuentas de ahorro y tarjetas de crédito y los saldos de 21.129 cuentas, en total habrían sido afectadas más de un millón de personas. Una vez ocurrido el incidente

el banco activó sus protocolos para casos de intrusiones informáticas e informó a las personas afectadas indicándoles que sus cuentas y tarjetas se bloquearon preventivamente. (Resolución Directoral N.° 1169 -2020-JUS/DGTAIPD-DPDP, 2020)

La Dirección de Fiscalización e Instrucción de la ANPD de Perú decidió iniciar un proceso administrativo sancionatorio contra el BCP por: i) no haber generado ni mantenido registro de interacción lógica sobre la base de datos del BCP, conforme lo exige el Reglamento de la LPDP; y ii) por no haber garantizado la confidencialidad de los datos personales de sus clientes, lo que viola el artículo 17 de la LPDP, que contiene la obligación de confidencialidad incluso luego de terminada la relación con el Titular. Vale aclarar que el registro de interacción de la base de datos documenta cómo interactúan los sistemas, aplicaciones y usuarios de una plataforma informática. Esto contiene información de registros de acceso, logs y autenticación, registros de transacciones, trazabilidad de las sesiones de los usuarios, eventos del sistema —como errores, caídas o anomalías— e interacción del sistema con otros, por ejemplo, a través de APIs.

Con relación a la primera imputación, la Dirección de Protección de datos Personales señaló que la obligación de mantener el registro de interacción lógica, contrario a lo alegado por el BCP, garantiza la seguridad de los datos y, concretamente, permite evidenciar qué usuario ingresó al sistema, en qué momento, qué operación realizó en el mismo y cómo lo hizo, y así establecer cuál fue el manejo de la información (Resolución Directoral N.° 1169 -2020-JUS/DGTAIPD-DPDP, 2020). La Dirección concluyó que esta obligación se incumplió por parte del BCP porque la infraestructura implementada al momento del incidente no permitía monitorear todas las actividades, aunque la sanción a imponer se subsumió junto con la correspondiente al incumplimiento al deber de preservar la confidencialidad de los datos (Resolución Directoral N.° 1169 -2020-JUS/DGTAIPD-DPDP, 2020).

La discusión acerca de la violación al deber de confidencialidad en este caso resulta interesante porque el BCP alegaba que este no se habría incumplido porque, según su postura, la norma solo contempla dos supuestos de incumplimiento: i) que haya una difusión consciente por parte del Responsable; o ii) una omisión de seguridad relevante al interior de la organización; no cabe dentro de estos supuestos el actuar temerario y malintencionado de un tercero a través de un ataque cibernético, de forma que el BCP no habría incumplido con el deber de confidencialidad.

Por el contrario, la Dirección consideró que la confidencialidad está estrechamente ligada con la seguridad, que no puede "garantizarse la primera sin la implementación de medidas técnicas, organizativas y legales preventivas a los riesgos conocidos e inherentes de toda actividad relacionada a sistemas y/o servicios informáticos" en la que se tratan datos personales.

Nótese que, siguiendo la postura de la Dirección, los ataques cibernéticos implican un riesgo inherente al tratamiento de datos por medios informáticos, y que es deber del Responsable garantizar a toda costa que no se presenten esos incidentes porque de manera automática va a estar incumplimiento no solo con el deber de seguridad, sino también el de confidencialidad. Aunque debe destacarse que en este caso la Dirección sí tuvo en cuenta que el BCP utilizó un aplicativo que no cumplía con sus propios estándares de seguridad; que no implementó controles para identificar a las personas que realizaban acciones sobre el aplicativo; que la metodología usada en el desarrollo del aplicativo no estaba diseñada para minimizar la posibilidad de vulneraciones al sistema; y que ya se habían presentado vulneraciones similares sin que se hubieran implementado correctivos, lo que evidencia negligencia (Resolución Directoral N.° 1169 -2020-JUS/DGTAIPD-DPDP, 2020,)[5].

Otro caso que se presentó en Perú y que resulta de interés para el presente análisis corresponde al resuelto el 14 de febrero de 2022 sobre la circulación de datos personales, incluso sensibles, entre personal de control migratorio en el aeropuerto de Jorge Chávez en Callao. Los funcionarios de la Superintendencia Nacional de Migraciones tomaban datos y fotos tanto de nacionales peruanos como de extranjeros y las compartían por WhatsApp. Además, en las computadoras de los módulos de control migratorio se encontraron puertos USB y equipos para grabar DVD, entre otros hallazgos, que darían cuenta de la violación del deber de confidencialidad y la falta de medidas de seguridad de los datos personales pues no se restringía la copia y reproducción de los mismos.

Aunque, para el momento de la Resolución Directoral N.° 655-2022, mediante la cual se resolvió el caso, la normativa peruana aún no contaba con una norma que consagrara expresamente el principio de responsabilidad proactiva, la Dirección de Protección de Datos Personales lo destacó en

5 Otro aspecto interesante de este caso fue la medida correctiva impuesta por la DPDP al BCP consistente en el cambio de los números de tarjeta de todos los Titulares afectados por el incidente. El BCP alegaba que esa medida era improcedente porque ya el incidente se había producido, de forma que la afectación a la seguridad era un hecho consumado y la medida correctiva resultaba desproporcionada y mucho mayor que la multa. Estos alegatos fueron rechazados en apelación (Resolución Directoral N.° 49-2020-JUS/DGTAIPD, 2020).

su decisión como un mecanismo para garantizar la seguridad de los datos biométricos que se emplean para la identificación de las personas en los procesos migratorios. Asimismo, fundamentó este principio como un elemento de la privacidad por defecto y por diseño contemplado en la GDPR Europeo y los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Resolución Directoral N.° 655-2022-JUS/DGTAIPD-DPDP). Así, la Resolución Directoral N.° 655 de 2022 señala:

> Ambas disposiciones responden de forma común a la necesidad de establecer obligaciones de prevención, a concretarse con actuaciones proactivas de parte de quien realiza el tratamiento de datos personales, encaminadas al cumplimiento de las obligaciones normativamente previstas y a la observancia de los Titulares de los datos personales, debiendo garantizar que el empleo de las herramientas de tratamiento, se ajusten a tales disposiciones y cumplan los objetivos de protección de derechos.
>
> En especial, la privacidad o protección de datos personales por defecto establece entre las cualidades esperadas de un tratamiento lícito, la limitación de la accesibilidad a los datos personales, evitando el acceso de una cantidad indeterminada de personas o el acceso por parte de quienes no requieren conocer los datos personales para cumplir con sus funciones; además de aplicar tal limitación según el criterio de minimización del tratamiento a lo necesario para alcanzar sus finalidades, acordes a las funciones de cada entidad (p. 14).

Con relación a la falta de medidas de seguridad que impidieran que los datos biométricos fueran reproducidos por los funcionarios, la Superintendencia Nacional de Migraciones estableció un procedimiento para restringir la copia de los datos asignando privilegios solo a determinados usuarios que podrían emplear los puertos USB, lectores de DVD, correos y celulares. En el proceso se determinó su implementación estaba pendiente y fue una de las medidas correctivas establecidas en la Resolución Directoral N.° 655-2022.

4.4. México

En México, la Ley de Protección de Datos Personales, la Ley General de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) fue modificada en el 2025. Uno de los principales cambios fue la desaparición del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), que actuaba como ANPD, y su cambio por la Secretaría Anticorrupción y Buen Gobierno.

La LFPDPPP de 2010 contemplaba, en su artículo 14, el principio de responsabilidad, por el cual los Responsables debían velar por el cumplimiento de los principios establecidos en la ley y adoptar las medidas necesarias para su aplicación. Este mismo principio se encuentra en el artículo 13 de la LFPDPPP de 2025. No obstante, debe resaltarse que no se especifica en este principio que el Responsable deba estar en capacidad de demostrar que implementó medidas dirigidas o necesarias para cumplir con sus obligaciones, en caso de ser requerido por la autoridad competente o por el Titular.

Igualmente, el principio de seguridad, que estaba en los artículos 19 y 20 de la LFPDPPP de 2010, se encuentra en los artículos 18 y 19 de la ley actualmente vigente. Estos artículos establecen que el Responsable debe implementar las medidas administrativas, técnicas y físicas para proteger los datos de daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado. Como parámetro, se establece que las medidas a adoptar no sean menores a las que el Responsable usa para el manejo de su información, que deberá tener en cuenta el riesgo existente y las eventuales consecuencias para los Titulares. El artículo 19 de la LFPDPPP de 2025 señala que se debe informar al Titular de las vulneraciones a la seguridad que se presenten en cualquier fase del tratamiento y que afecten de forma significativa sus derechos patrimoniales o morales.

En el 2020 se publicó, sin medidas de seguridad, una base de datos de 830.000 servidores públicos de la Secretaría de la Función Pública. Los datos que pudieron accederse libremente incluían nombres, experiencia laboral, ingresos, bienes muebles e inmuebles, vehículos, inversiones, deudas y préstamos entre otros. La entonces autoridad competente, el INAI, inició una investigación y concluyó que se violaron los deberes de confidencialidad y seguridad de los datos personales, pues no se implementaron medidas para evitar accesos no autorizados y prevenir riesgos previsibles (Resolución INAI.3S.07.01.005/2020). Aunque el motivo del incidente fue un factor externo a la Secretaría, este no fue tenido en cuenta como un fundamento legítimo de defensa porque la Secretaría no acreditó haber implementado controles y mecanismos de seguridad adecuados.

Un caso de gran relevancia en México fue el de MercadoLibre. En marzo de 2022, la prensa informó de un ciberataque a la plataforma de comercio electrónico por el que se habrían filtrado datos de 300.000 personas y código fuente de la compañía. La empresa admitió que el ataque se presentó en un Encargado contratado por una empresa del grupo para realizar actividades que requerían el tratamiento de datos. Una vez se presenta el incidente, Mercado Libre activó sus protocolos de ciberseguridad y, dentro de las medidas tomadas, notificó a los Titulares del incidente y publicó información en

su página web. El INAI tuvo conocimiento del incidente que afectó a 171.593 Titulares mexicanos; la mayoría de los datos vulneraros permitirían el contacto con el Titular pues correspondían a correos y números telefónicos pero la información financiera no se habría visto afectada (Resolución ACT-Priv/19/11/2022.04.01.0736, p. 143).

Como parte de sus consideraciones, el INAI precisó las actividades que deben implementar el Responsable para cumplir con el principio de seguridad:

> A fin de establecer y mantener la seguridad de los datos personales, el Responsable y el Encargado respectivamente deberán considerar obligatoriamente las siguientes acciones: i) elaborar un inventario de datos personales y de los sistemas de tratamiento; ii) determinar las funciones y obligaciones de las personas que traten datos personales; iii) contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales; iv) establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva; v) realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales; vi) elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha; vii) llevar a cabo revisiones o auditorías; viii) capacitar al personal que efectúe el tratamiento, y; ix) realizar un registro de los medios de almacenamiento de los datos personales. Además, el Responsable deberá contar con una relación de las medidas de seguridad derivadas de las fracciones anteriores (Resolución ACT-Priv/19/11/2022.04.01.0736, pp. 169-170).

Ahora bien, es importante destacar que el INAI consideró como una confesión el comunicado emitido por Mercado Libre sobre el tratamiento de datos personales de ciudadanos mexicanos, del tratamiento de los datos por parte de la empresa del grupo constituida en México y del acaecimiento del incidente de seguridad (Resolución ACT-Priv/19/11/2022.04.01.0736, p. 171).

Sin embargo, en un análisis de las medidas implementadas una vez ocurrido el hackeo el INAI resalta que MercadoLibre no demostró haber realizado un análisis de riesgos referentes al tratamiento de los datos personales que incluyera la identificación de los peligros, la estimación de los riesgos, la determinación de los controles y medidas de seguridad para su mitigación, por lo que "al no contar o no presentar un análisis de riesgo no es posible determinar si las medidas de seguridad establecidas eran las aplicables a los datos personales y sistemas de tratamiento" (Resolución ACT-Priv/19/11/2022.04.01.0736, p. 183).

Adicionalmente, el INAI destacó que los documentos allegados para probar la implementación de medidas de seguridad, tanto por el Responsable como por terceros encargados que participaban en el tratamiento de los datos, fueron insuficientes porque se trataba de meras políticas o conjunto de orientaciones y directrices, pero no se evidenció que las mismas se hubieran implementado. Por ello, se concluyó que la plataforma de comercio electrónico incumplió con su deber de seguridad.

Dos Comisionadas del INAI presentaron su disenso frente a la decisión adoptada por el APDP de México. La Comisionada Presidenta se apartó de la decisión mayoritaria argumentando que no se demostró que el Responsable divulgara la información, sino que la divulgación se debió a la vulneración de seguridad "consistente en un acceso no autorizado por parte de un tercero", por ello, "no puede considerase que el Responsable incumplió el deber de seguridad." Agregó la Comisionada Presidenta que:

> Lo anterior no significa que el Responsable esté exceptuado de responsabilidad; sin embargo, era necesario delimitar la misma conforme a la conducta probada, relacionada con el principio de responsabilidad y el establecimiento de las medidas de seguridad necesarias (Ibarra, 2022).

También emitió un voto particular otra Comisionada quien sostuvo que el INAI no satisfizo la carga de demostrar fehacientemente que fue el Responsable quien en incumplimiento del deber de confidencialidad divulgara los datos personales, patrimoniales o financieros de los Titulares. Esto porque no se demostró que existiera un vínculo o relación entre las páginas donde se divulgó la información y el Responsable; tampoco que hubiera vulnerado las medidas de seguridad de las bases de datos. Así, no podría concluirse que el Responsable incumplió el deber de seguridad. Sobre todo porque el artículo 63- XI de la LFPDPPP de 2010 establece que es una infracción a la misma norma el vulnerar la seguridad de las bases de datos cuando resulte imputable al Responsable.

Retomando lo señalado antes sobre el PRD, que en sí mismo exige la evaluación de riesgos para identificar las medidas de seguridad que deben adoptarse en cada caso concreto, la postura del INAI es bastante acertada justamente porque exigió tal análisis y la prueba de que las políticas de seguridad hubieran pasado del papel a la práctica. Sin embargo, los votos particulares de las dos Comisionadas reiteran que el mismo incidente de seguridad se tiene como prueba infalible del incumplimiento del deber de seguridad y confidencialidad de los datos, aunque la vulneración a las medidas de seguridad y la divulgación la hubiera realizado un tercero.

4.5. Algunas anotaciones

De los casos antes referidos es evidente la diversidad existente en la región en la aplicación del PRD y el deber de seguridad de los Responsables. Por supuesto, aunque teóricamente el PRD y el deber de seguridad en el tratamiento de datos personales puedan tener fuentes u orígenes comunes en Latinoamérica, existen importantes diferencias en su aplicación a casos concretos.

En Colombia hay casos en los que se presume, por el simple hecho de existir el incidente de seguridad, que hubo un incumplimiento en las obligaciones del Responsable y, sin analizar las medidas de seguridad adoptadas ni la forma en que ocurrió el incidente, se ordena reforzar las medidas —esto en las Resoluciones citadas de 2021-2023—. Esto muestra una clara contradicción con lo que señalan las normas del país que apuntan a que la aplicación del PRD y el deber de seguridad sea contextual y proporcional al riesgo. En contraste, en casos más sonados —como el de UBER y ScotiaBank— sí se efectúo un análisis de los incidentes con fallas concretas en las medidas de seguridad, como falta de autenticación multifactor, alarmas en los sistemas por correos enviados a cuentas comerciales, control de privilegios y excepciones al DLP, lo que permitió identificar por qué las medidas fueron insuficientes.

En Perú, el PRD no fue implementado originalmente en su Ley de Protección de Datos Personales, sino que, al igual que en Colombia, fue consagrado explícitamente con posterioridad a través de normas complementarias —Decreto Supremo N.° 16 de 2024—. Adicionalmente, el Reglamento Peruano contine unos mínimos de seguridad que han permitido analizar el cumplimiento del deber de seguridad en casos concretos, como en el caso del BCP, con la ausencia del registro de interacción lógica, que permitiría demostrar quién, cuándo y cómo accedió a los sistemas y qué hizo en ellos. Además, en esta decisión se resaltan otras falencias en el sistema como la metodología de desarrollo, controles insuficientes. Por su parte, el caso de la Superintendencia Nacional de Migraciones introduce explícitamente una lógica de prevención/proactividad y limitación de accesibilidad, es decir, la privacidad por defecto/diseño como parte del estándar exigible.

En México, es destacable la postura adoptada por el extinto INAI en el caso de Mercado Libre, pues, si bien se tomó como confesión el haber informado del incidente públicamente no se adoptó una postura que partiera de la existencia del hackeo para sancionar. Por el contrario, se estudió con fundamento en las pruebas el deber de seguridad exigiendo un análisis de riesgos y la implementación práctica de las medidas documentadas. Sin embargo, los votos particulares de las Comisionadas del INAI evidencian diferencias en cuanto a la imputación de la responsabilidad por los incidentes de seguridad. Mientras que la mayoría del INAI considera que una violación a las medidas de seguridad por un tercero conlleva una violación al deber de confidencialidad, también las Comisionadas plantean una postura que se comparte en el sentido de que quien viola la confidencialidad no es el Responsable, sino el terceo.

Brasil es una jurisdicción particular porque ha elaborado una doctrina de una expectativa legítima de seguridad en favor del Titular. Esta expectativa de seguridad se analiza considerando las técnicas de tratamiento disponibles, la previsibilidad de las actuaciones, la velocidad con la que deben implementarse actualizaciones disponibles en esta materia. Ahora bien, según esta expectativa de seguridad, el Responsable sólo puede eximirse de responsabilidad si demuestra que el incidente fue *culpa exclusiva del tercero atacante*, lo cual también es una prueba diabólica en sí misma. porque como se dijo, en seguridad informática siempre existirá el riesgo residual.

Un punto común que emerge en los cuatro países es la ambigüedad de la palabra "efectivas" con relación a las medidas de seguridad y a la expectativa legítima de seguridad del Titular. Si por "efectivo" se entiende como aquella medida "capaz de impedir todo ataque", entonces la seguridad se convierte en una obligación de resultado incompatible con el riesgo residual y con el PRD que, al menos en teoría, debe ser proporcional al tipo de datos tratados, a los estándares técnicos, a los riesgos para el Titular e incluso a las capacidades económicas del Responsable. Si, en efecto, se exige que las medidas puedan impedir todo ataque se pueden presentar dos efectos adversos que se alejan de lo que las normas pretenden lograr:

- **Incentivos perversos**: si cualquier incidente demuestra insuficiencia de las medidas, el PRD deja de ser una obligación de medios o de gestión (frente a un riesgo actuar con diligencia) y se vuelve una carrera imposible. En ese escenario, tiene sentido económico desplazar recursos hacia mecanismos *ex post* (como seguros, gestión reputacional, notificación) en lugar de invertir incrementalmente en prevención.
- **Desalineación con la proporcionalidad**: tanto Colombia y Perú, por disposición normativa, como México y Brasil, por criterio/estructura, reconocen que el estándar depende de factores como naturaleza de los datos, alcance, riesgos, tamaño/recursos y estado de la técnica. Si, aun así, se presume responsabilidad solo por la ocurrencia del incidente, esos factores quedan vacíos y ello desnaturaliza el PRD.

Entonces, la "efectividad" de las medidas debe evaluarse *ex ante*, como razonabilidad de controles frente al riesgo y el contexto, y *ex post* para evaluar la calidad de la respuesta del Responsable frente al incidente, por ejemplo, que medidas de contención adoptó, si era procedente la notificación a los Titulares y se realizó correctamente, si realizó una evaluación de lo sucedido e implementó controles y correcciones adecuadas.

Otro asunto que se planteó es la posibilidad de que en ciertas circunstancias los ciberataques se consideren como causales eximentes de responsabilidad. De los casos analizados en las cuatro jurisdicciones se plantean tres escenarios que permitirían evaluar esta posibilidad:

1. **Improcedencia porque en el incidente se presentó una falla en una medida de seguridad que puede ser atribuible al Responsable**: cuando el incidente se vincula con controles ausentes o deficientes, o con omisiones previsibles. Por ejemplo, privilegios sin monitoreo, ausencia de autenticación multifactor donde es razonable, falta de logs o trazabilidad mínima en los sistemas, herramientas fuera de estándar interno, ausencia de análisis de riesgos. En los casos en los que esto se demuestre con pruebas en el proceso, es evidente que el ataque de un tercero revela una vulnerabilidad no gestionada.

2. **Exime condicionada a que se demuestre que el Responsable actuó diligentemente y hubo un ataque irresistible**: cuando el Responsable demuestra documental y técnicamente que realizó análisis de riesgos, seleccionó controles razonables y actualizados, auditó/monitoreó, y aun así ocurrió un ataque sofisticado no previsible o no resistible en ese contexto. En este escenario, el PRD opera debidamente a que el Responsable demuestra diligencia y que actuó de forma razonable y proporcional a su evaluación de riesgos. Además, se debe evaluar la irresistibilidad del ataque. Entonces, la consecuencia debería ser, al menos en sede administrativa, un tratamiento diferenciado que no conlleve directamente a la sanción por la existencia del incidente sino solicitar medidas correctivas y su implementación real.

3. **Exime por culpa exclusiva de tercero**: aplicaría cuando, además de lo anterior, el incidente se deba a un hecho totalmente externo y extraordinario, sin vulneración de controles razonables por parte del Responsable. Aquí el estándar es alto (como en Brasil), pero debe entenderse como una excepción, no como vía ordinaria para escapar de responsabilidad.

Este enfoque tripartito permite reconciliar el PRD con el deber de seguridad pues no "castiga automáticamente por existir un incidente", sino que obliga al Responsable a poder demostrar (i) que gestionó riesgos antes; y (ii) que actuó diligentemente después.

5. ¿El Estado tiene alguna obligación de policía en Internet?

Una inquietud final, que simplemente será planteada acá para futuras consideraciones es si cabe al Estado alguna obligación de policía en Internet frente a casos de ciberataques. En el mundo análogo, cuando se presenta un hurto de un bien tangible por lo general los esfuerzos del Estado se concentran en encontrar y castigar al ladrón. En el mundo digital ha imperado una postura un poco diferente, como se señaló antes, se ha partido de que estas actividades en Internet tienen implícito un riesgo de ataques por parte de terceros que, como pueden afectar a un consumidor, usuario Titular de datos personales que poco o ningún control tiene sobre la situación debe ser protegido y como es muy difícil encontrar a los hackers, entonces los Responsables que adelantan esas actividades peligrosas deben, por todos los medios, proteger a la parte débil o serán sancionados. Entonces, ¿dónde queda la obligación de buscar y castigar al ladrón/hacker en el Internet?

Por supuesto, la doctrina ya ha abordado esta cuestión e incluso los Estados han implementado mecanismos para incrementar la seguridad en Internet. El Estado tiene un deber general de proteger a sus ciudadanos, en gran parte es fundamento de la existencia misma de los Estados como establecieron Locke y Hobbes. Ese deber de cuidado y protección no se queda sólo en el entorno análogo, sino que se proyecta en igual medida en el digital (Shore, 2015), el cual también tiene efectos reales en la vida de las personas. Esto explica muchas medidas y políticas para proteger infraestructura crítica para la seguridad nacional y también un deber compartido con agentes privados de perseguir la criminalidad en Internet (Shore, 2015).

Así, los Estados han elaborado y están implementando políticas dirigidas a controlar la ciber criminalidad. Un ejemplo de ello se halla en el Plan Nacional de Desarrollo 2022-2026 y la Estrategia Nacional Digital 2023-2026 en Colombia, donde se subraya la importancia de fortalecer la institucionalidad de la seguridad digital del país. Otros países, como Estados Unidos, ya cuentan con agencias como la Agencia de Ciberseguridad y Seguridad de las Infraestructuras del Departamento de Seguridad Nacional de los Estados Unidos Responsable de la ciberseguridad y la protección de las infraestructuras del gobierno. Incluso el

Convenio sobre cibercriminalidad de Budapest reconoce la obligación de los estados de investigar y sancionar los delitos informáticos.

Sin embargo, hay quienes van más lejos aún y expanden la responsabilidad del Estado de un mero agente que prohíbe ciertas conductas que son perjudiciales para la sociedad a obligaciones de hacer que implican medidas preventivas, acciones de respuesta frente a incidentes y deberes de reparación (Putri & Nathanael, 2026). En parte la justificación o el motivo por el cual se espera mayor proactividad de los Estados frente a los ciberataques es que estos tienen estructuras e impacto transnacional, por lo que la fijación de estándares y actuación coordinada entre diferentes agentes requieren participación de entes públicos (Wall, 2007) con mayores capacidades de convocatoria, agencia y vinculatoriedad.

6. Conclusiones

1. Tanto el PRD como el deber de seguridad fueron ideados para pasar de un cumplimiento de requisitos burocráticos —como publicar una política de tratamiento, un manual interno o inscribirse en un Registro Nacional de Bases de Datos— a un cumplimiento más real y efectivo que realmente tuviera en cuenta las actividades de tratamiento que se realizan sobre los datos personales y como esas actividades pueden afectar los derechos de los Titulares. Sin embargo, ninguno de esos principios o normas es prospectivo, es decir, ninguno establece de forma concreta qué medidas deben implementarse para cumplir con ellos, sino que su materialización debe realizarse a partir de una evaluación de los riesgos que genere el tratamiento a los derechos de los Titulares y otras circunstancias como: el tipo y volumen de datos tratados, los estándares de seguridad vigentes y los recursos del Responsable. De forma que no existe un parámetro concreto para la aplicación del PRD ni del deber de seguridad.

2. En muchos de los casos analizados el mismo incidente de seguridad se tiene como prueba del incumplimiento de los deberes de seguridad y en pocos casos se ha sopesado si las medidas implementadas eran razonables o proporcionales a la evaluación de riesgo con fundamento en las pruebas allegadas al proceso. Esto porque la efectividad de las medidas de seguridad se equipará a una medida "capaz de impedir todo ataque." En consecuencia, se reduce la seguridad jurídica respecto de la posibilidad de que realmente realizar una evaluación de riesgos y desarrollar medidas de seguridad consecuentes puedan reducir o eximir de sanciones al Responsable y estimula la inversión en seguros, notificaciones y contención del riesgo reputacional, ocasionando un efecto contrario al deseado con el PRD.

3. Una verdadera evaluación del deber de seguridad basado en el PRD debería analizar *ex ante* la razonabilidad de las medidas frente a los riesgos identificados y ex post analizar la calidad de la respuesta frente al incidente, la efectividad de las medidas de contención, la oportunidad en la información a la autoridad y a los Titulares, así como la verdadera implementación de correctivos.

4. Con relación a los ciberataques como eximentes de responsabilidad y de sanciones, basados en los casos analizados de Colombia, Brasil, Perú y México en los que la ocurrencia de un incidente de seguridad casi que automáticamente conduce a sanciones, se planeó un análisis tripartito que permitiría evaluar esta posibilidad considerando la diligencia de los Responsables en la implementación de medidas de seguridad. Así, si el ataque cibernético se debe a una falla en las medidas de seguridad que sea atribuible al Responsable, naturalmente el incidente no lo eximiría de responsabilidad. Por el contrario, si el Responsable actúa diligentemente e implementa medidas acordes al nivel de riesgo y se presenta un ataque sofisticado imprevisible e irresistible, debería eximirse de responsabilidad y evaluarse cómo actuó frente a la ocurrencia del incidente. Finalmente, en el tercer nivel, si ocurre un hecho totalmente externo y extraordinario que sea totalmente atribuible al tercero, se eximiría al Responsable de toda responsabilidad. Este último caso, sería por supuesto, aplicando un nivel de exigencia mayor como el aplicado en Brasil.

5. Este análisis aplicado a casos concretos, permite reconciliar el PRD con el deber de seguridad, pues no sanciona automáticamente ante la ocurrencia de un incidente, sino que obliga al Responsable a demostrar: (i) que gestionó riesgos antes, y (ii) que actuó diligentemente después. Asimismo, este enfoque obliga a las ANPD a evaluar con mayor detalle las causas del incidente de seguridad, las medidas de seguridad en busca de falencias que pudieran evitarse y la previsibilidad e irresistibilidad del ataque. De esta forma, se lograría el objetivo de la implementación del PRD, esto es, que las reglas y principios del tratamiento de datos personales, como la seguridad y la confidencialidad, se materialicen y actualicen conforme avanza la tecnología y las actividades de tratamiento.

6. Aunque la postura adoptada tendría su principal impacto en el análisis de la responsabilidad

administrativa de los Responsables frente a casos de incidentes de seguridad, desde la perspectiva regulatoria, el caso de Perú mostró que contar con una regulación que establezca aunque sea los mínimos de las medidas de seguridad que deben implementarse —como el registro de interacción lógica—, pues ello facilita evaluar las medidas de seguridad implementadas por el Responsable. Por supuestos, las normas técnicas que cada país aplique, los estándares reconocidos a nivel internacional, son también fundamento para este análisis. En todo caso, se requiere que las ANPD conozcan tales estándares y estén en capacidad de evaluarlos.

Lista de referencias

Alhadeff, V. A. (2012). The Accpuntability Principle in Data Protecion Regulation: Origin, Development and Future Directions. D. Guagnin, *et al. (eds.), Managing Privacy through Accountability*, 49-82.

Alsenoy, B. V. (2016). Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, *JIPITEC*, 271-288.

Alvarado, F. (2016). La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales. *Revista Foro Jurídico*, 26-41.

Antoni, C. F. (2022). Chapter 4: Cyber Security and the GDPR. In C. F. Antoni Gobeo, *GDPR and Cyber Security for Business Information Systems* (pp. 92-115). New York: River Publishers. https://doi.org/10.1201/9781003338253

Arenas, M. (2022). Data Protection in Latin America. In G. v. González-Fuster (ed.), *Research handbook on privacy and data protection law : values, norms and global politics.* (pp. 140-159). Edward Elgar Publishing.

Autoridade Nacional de Proteção de Dados (ANPD). (2023). Guia Orientativo – Segurança da Informação para Agentes de Tratamento de Pequeno Porte. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-public

Autoridade Nacional de Proteção de Dados. (2024). *Relatório de Instrução nº 1/2024/FIS/CGF/ANPD – Instituto Nacional do Seguro Social – INSS)*. https://www.gov.br/anpd/pt-br/centrais-de-conteu

Autoridade Nacional de Proteção de Dados. Brasília: ANPD. (2024). Relatório de Instrução nº 2/2024/FIS/CGF/ANPD – Processo nº 00261.001192/2022-14 (Secretaria de Estado de Educação do Distrito Federal – SEEDF). https://www.gov.br/anpd/pt-br/

Bennett, C. (2012). The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats. In D. H. Guagnin (ed.), *Managing Privacy through Accountability.* London: Palgrave Macmillan. https://doi.org/10.1057/9781137032225_3

Boonen, T., Feng, Y. & Tong, Z. (2025). Cibersecurity investments and cyber insurance purchases in a non-cooperative game. *ASTIN Bulletin: The Journal of the IAA*, 1-31. https://doi.org/10.1017/asb.2024.21

Brasil, Congreso Nacional. (2018, 14 de agosto). Lei Geral de Proteção de Dados Pessoais . *LGPD*.

Congreso de la República. (2012, 18 de octubre). Ley 1581 de 2012. *Por la cual se dictan disposiciones generales para la protección de datos personales.* Diario Oficial 48587.

Conselho Diretor da Autoridade Nacional de Proteção de Dados. (2024). Resolução CD/ANPD N.º 15/2024.

De Hert, P. & Lazcoz, G. (2022). When GDPR-principles blind each other: accountability, not transparency, at the heart of algorithmic governance. *European Data Protection Law Review, 8*(1), 31-40.

DGPDP Dirección General del Protección de Datos Personales. (2013, 11 de octubre). Resolución Directoral N.º 019-2013-JUS/DGPDP

Departamento Administrativo de la Función Pública. (2011, 23 de diciembre). Decreto 4886 de 2011. *Por medio del cual se modifica la estructura de la Superintendencia de Industria y Comercio, se determinan las funciones de sus dependencias y se dictan otras disposiciones.*

Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. (2020, 16 de noviembre). Resolución Directoral N.° 49-2020-JUS/DGTAIPD, Exp. 130-2019-JUS/DGTAIPD-PS.

Dirección de Protección de Datos Personales. (2022, 14 de febrero). Resolución Directoral N.° 655-2022-JUS/DGTAIPD-DPDP, Exp. 025-2021-JUS/DGTAIPD-PAS.

Dirección de Protección de Datos Personales. (2020,31 de julio). Resolución Directoral N° 1169 -2020-JUS/DGTAIPD-DPDP, Exp. 130-2019-JUS/DGTAIPD-PAS.

Eurostat. (2024, 26 de enero). How internet users protected their data in 2023. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240126-1?utm

Gardner, A. (2024). Who should be liable? Examinig the corporate Liability Regime of Cybersecurity Risks. *Priv. L.*, (2), 36-50 https://digitalcommons.mainelaw.maine.edu/sjipl/vol2/iss1/4

Ibarra, B. L. (2022). Voto Particular de la Comisionada Presidenta Blanca Lilia Ibarra. *Expediente de Verificación INAI.3S307302-049/2022*.

Instituto Nacional De Transparencia, Acceso a la Información y Protección De Datos Personales. (2022). Resolución ACT-Priv/19/11/2022.04.01.0736, Expediente de Verificación: INAI.3S.07.02-049/2022.

Instituto Nacional De Transparencia, Acceso a la Información y Protección De Datos Personales. (2020). Resolución INAI.3S.07.01.005/2020.

Jiménez, W. (2025). La responsabilidad objetiva de los bancos en los casos de fraude electrónico en Colombia. *Revista Misión Jurídica*, *18*(28), 127-153.

Koolen, C., Wuyts, K. & Jossen, W. (2024). From insight to compliance: Appropiate technical and organisational security measures through the lens of cybersecurity maturity models. *Computer Law & Security Review,* 1-10.

Macenaite, M. (2017). The "Riskification" of the European Data Protectioon Law through a two-fold Shift. *European Journal of Risk Regulation*, *8*(3), 506-540.

Mantelero, A., Vaciago, G. & María, E. (2020). The Common EU Approach to Personal Data and Cybersecurity Regulation. *Internation Jpurnal of Law and Information Technology*, 297-328.

McClain, C., & Faverio, M. (2023, Octubre 18). How Americans View Data Privacy. *Pew Researche Center, 8*(4), *297-328*. Retrieved from https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/?utm

Ministerio de Justicia y Derechos Humanos. (2018, 12 de enero). Oficio No. 65 . *Absolución de consulta en Materia de medidas de seguridad*.

Ministerio de Justicia y Derechos Humanos, Perú. (2024, 30 de noviembre). Decreto Supremo N.° 16 de 2024. *Diario Oficial El Peruano*.

OECD. (2002). Directrices sobre la protección de la privacidad y los flujos transfronterizos de datos personales. Paris: OECD Publishing. https://doi.org/10.1787/9789264196391-en.

Oficina del Alto Comisionado de las Naciones Unidas. (2022). Principios que informan la privacidad y la protección de datos personales (Documento A/77/196).

Petry, G. C., Rick, K. & Engelmann, W. (2025). Security Incidents, Data Leaks and Cyber Attacks: Possible Answers for the Application of the Law Based on the STJ'S Decisions In Resp 2.147.374/Sp and Aresp 2.130.619/Sp. *Revista Direito Mackenzie*.

Putri, S. & Nathanael, K. (2026). Digital Vulnerability and the Expansion od State Responsibility in Data Protection and Cyber Governance. *Qriset Indonesia Journal of Law, 1*(1), 39-47.

Quelle, C. (2017). The 'risk revolution' in EU data protection law: We cant have our cake and eat it, too. In R. Leenes, R van Brakel, S. Gutwirth & P. De Hert (eds.), *Tilburg Law School Legal Studies Research Paper Series*. Hart Publishing.

Quelle, C. (2018). Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach. *European Journal of Risk Regulation, 9*, 502-526.Riaño, A. (2023). Reflexiones en torno a la adaptación de la responsabilidad objetiva en el marco del tratamiento de datos personales. En E. Corteés, & M. C. M'causland, *La Responsabilidad Objetiva entre esquemas tradicionales y nuevas realidades* (pp. 178 - 225). Universidad Externado de Colombia.

Sánchez, I., San, T & Calvo-Manzano, J. (2023). Countermeasures and their taxonomies for risk treatment in cybersecurity. *Computers & Security*.

Selzer, A. (2021). The appropriateness of technical and organisational measures. *European Data Protection Law Review*, *7*(1), 120-128.

Shore, J. (2015). An obligation to Act: Holding Government Accountable for Critical Insfrastructure Cyber Security. *International Journal of Intelligence and CounterIntelligence*, *28*(2), 236-251.

Solove, D. (2026). *Enforcing Privacy Law: Why private litigation is essential.* George Washington University Law School.

Superintendencia de Industria y Comercio. (2025, 12 de setiembre). Resolución 70035 de 2025, Exp. 22-416065.

Superintendencia de Industria y Comercio. (2023, 28 de julio). Resolución 43407 de 2023, Exp. 20-120413.

Superintendencia de Industria y Comercio. (2023, 28 de julio). Resolución 43249 de 2023, Exp- 20-120420.

Superintendencia de Industria y Comercio. (2023, 28 de julio). Resolución 43325 de 2023, Exp. 20-120410.

Superintendencia de Industria y Comercio. (2022, 28 de octubre). Resolución 75732 de 2022, Exp. 20-30059.

Superintendencia de Industria y Comercio. (2022, 10 de octubre). Resolución 70773 de 2022, Exp. 18-175769.

Superintendencia de Industria y Comercio. (2022, 10 de octubre). Resolución 70784 de 2022, Exp- 18-345513.

Superintendencia de Industria y Comercio. (2022, 10 de octubre). Resolución 75741 de 2022, Exp. 19-123001.

Superintendencia de Industria y Comercio. (2021, 30 de junio). Resolución 40704 de 2021, Exp. 20-120563.

Superintendencia de Industria y Comercio. (2019). Resolución 21478 de 2019, 2019-40311.

Superior Tribunal de Justicia de Brasil. (2025, 18 de junio). AREsp 2.170.495/SP.

Superior Tribunal de Justicia. (2025, 2 de noviembre). REsp 2.121.904/SP (STJ, 3ª Turma, 2024/0031292-7.

Superior Tribunal de Justicia. (2024, 3 de diciembre). REsp 2.147.374/SP (STJ, 3ª Turma, REsp 2.147.374/SP.

Superior Tribunal de Justicia de Brasil. (2023, 26 de setiembre). Recurso Especial N.º 2.077.278 - SP, (2023/0190979-8).

Superior Tribunal de Justicia. (2023, 7 de marzo). AREsp N.º 2.130.619-SP.

Superintendencia de Industria y Comercio. (2020). *Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales.*SIC.

Superintendencia de Industria y Comercio. (n.d.). *Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability).* SIC. Tacha, P. (2024). Los Ciberataques como eximientes de responsabilidad civil del encargado y Responsable del tratamienot de datos prsonales en entidades privadas. *Tesis Maestría en Derecho Privado, Persona y Sociedad*. Universidad Externado de Colombia .

Tschider, C. (2023). Locking down "Reasonable" Cybersecurity Duty. *Yale Law & Policy Review*, *41*(2), 75- 151.

Vásquez, R. (2022). La responsabilidad protactiva en la normativa peruana de protección de datos personales. *Revisata de Derecho YACHAQ., 13*, 25-37.

Wall, D. S. (2007). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. *Police Practice and Research*, *8*(2), 183-205. https://doi.org/10.1080/15614260701377729