15 Noviembre, 2026

Caso Interbank establece precedente para exonerar multas por filtraciones de datos

La Autoridad Nacional de Protección de Datos Personales determinó, en primera instancia, que Interbank fue responsable de la filtración de información privada de sus clientes en un ciberataque ocurrido en 2024, en el que se extrajeron 1,8 millones de registros de sus clientes. Sin embargo, la resolución de este caso estableció un nuevo criterio en la aplicación de sanciones que permitirá eximir del pago de multas a las empresas, incluso después de una filtración masiva de información. La actual gestión de la autoridad presentó este cambio ante empresarios de la Cámara de Comercio Americana del Perú (AmCham Perú).

Por Fiorella Montaño



FILTRACIÓN MASIVA: La investigación de la Autoridad de Datos Personales identificó deficiencias en los sistemas de seguridad que facilitaron el robo de información.

Foto: ANDINA / Editora Perú

El robo y la filtración de datos personales de clientes ya no implican necesariamente una multa para las empresas responsables de proteger esa información. Desde el 23 de setiembre de este año, la Autoridad Nacional de Protección de Datos Personales (ANPD) aplica un nuevo criterio para sancionar las infracciones relacionadas con la seguridad de los datos. El cambio surgió a raíz de la investigación de un **ciberataque a Interbank**, que expuso información privada de sus clientes en 2024.

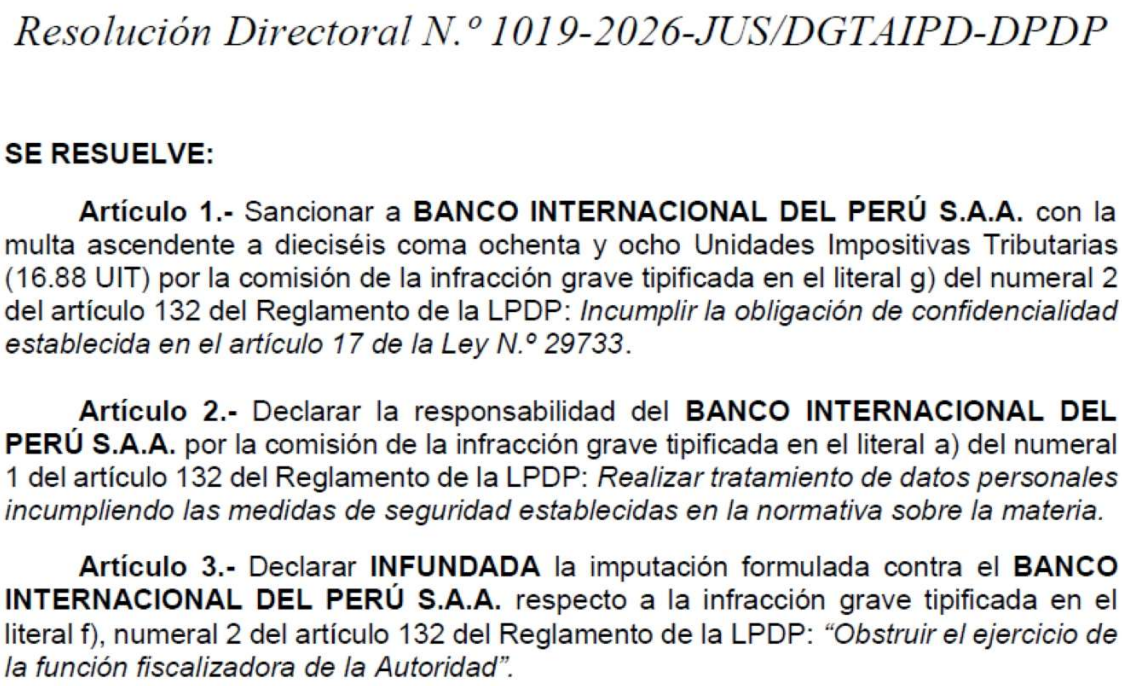
Hazte Aliado/a

En setiembre de ese año, un hacker ingresó a los sistemas de Interbank (Banco Internacional del Perú S.A.A.) y descargó 1,8 millones de registros de clientes. La información incluía números de DNI, direcciones, correos electrónicos, números de cuenta e incluso datos sobre la marca, el modelo, el código IMEI y la geolocalización de sus celulares. La filtración se hizo pública el 30 de octubre del mismo año, cuando el usuario Kzoldyck anunció que tenía los datos a la venta en un foro de la dark web.

> ***EN SETIEMBRE DE 2024, UN HACKER INGRESÓ A LOS SISTEMAS DE INTERBANK Y DESCARGÓ 1,8 MILLONES DE REGISTROS DE CLIENTES.***

La Autoridad Nacional de Datos Personales inició una investigación en octubre de 2024 y, casi dos años después, mediante la Resolución Directoral 1019-2026, determinó, en primera instancia, que Interbank cometió dos infracciones graves a la Ley de Protección de Datos Personales: “incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley 29733” y “realizar el tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia”.

Además, impuso al banco una multa de S/86.932, correspondiente a 16.88 UIT con el valor de 2024. De no apelar la sanción, Interbank puede acceder a una reducción de más de S/34.000. El artículo 9 de la resolución analizada por este medio indica que el banco "puede acogerse al beneficio de pronto pago de la multa", que consiste en la reducción del 40% del monto total.



Resolución Directoral N.º 1019-2026-JUS/DGTAIPD-DPDP

SE RESUELVE:

Artículo 1.- Sancionar a **BANCO INTERNACIONAL DEL PERÚ S.A.A.** con la multa ascendente a dieciséis coma ochenta y ocho Unidades Impositivas Tributarias (16.88 UIT) por la comisión de la infracción grave tipificada en el literal g) del numeral 2 del artículo 132 del Reglamento de la LPDP: *Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley N.º 29733.*

Artículo 2.- Declarar la responsabilidad del **BANCO INTERNACIONAL DEL PERÚ S.A.A.** por la comisión de la infracción grave tipificada en el literal a) del numeral 1 del artículo 132 del Reglamento de la LPDP: *Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia.*

Artículo 3.- Declarar **INFUNDADA** la imputación formulada contra el **BANCO INTERNACIONAL DEL PERÚ S.A.A.** respecto a la infracción grave tipificada en el literal f), numeral 2 del artículo 132 del Reglamento de la LPDP: *“Obstruir el ejercicio de la función fiscalizadora de la Autoridad”.*

INFRACCIONES. La Resolución Directoral 1019, determinó que Interbank cometió dos infracciones graves a la Ley de Protección de Datos Personales.

Captura de documento

No es el único beneficio que se puede obtener. En la misma resolución directoral, se modificaron los requisitos para eximir de multas a las empresas que vulneren esta misma ley, incluso cuando se haya producido una filtración masiva de información.

Hasta entonces, explica la citada resolución directoral, para que una empresa lograra eximir una multa, era necesario que primero acreditara haber corregido su conducta, resarciera el daño producido y adoptara voluntariamente las medidas que fueran necesarias para restablecer el orden alterado.

El nuevo criterio de la autoridad establecido en dicha resolución considera que la exigencia de resarcir el daño creaba una categoría de multas que no podrían ser exoneradas. Siendo este el caso de las filtraciones.

Para permitir la exoneración de multas a empresas que sufrieron filtraciones, se establecieron tres nuevos requerimientos. El primero es corregir las acciones que dieron lugar a la infracción; el segundo, que la corrección se realice de forma voluntaria y el tercero, que las medidas correctivas se adopten antes de que la autoridad notifique al infractor la imputación

Hazte Aliado/a

Artículo 4.- Precisar que la Dirección ha adoptado un cambio de criterio con respecto a la eximente de responsabilidad por subsanación voluntaria, en los términos que se resumen a continuación:

> *El TUO de la Ley No. 27444 consagra como eximente de responsabilidad a la subsanación voluntaria del acto u omisión imputado como constitutivo de infracción administrativa con anterioridad a la notificación de la imputación de cargos. En ese sentido, para la aplicación de la eximente, se requiere la comprobación de tres elementos: (i) que se haya producido la subsanación plena del acto u omisión imputado y constitutivo de infracción. Al respecto, la Dirección entiende por subsanación a la adopción de medidas idóneas, ejecutadas y acreditadas que corrigen el acto u omisión originadora de la infracción; (ii) que sea voluntaria, esto es, que no responda a una orden concreta de la autoridad de realizar las medidas preventivas específicamente adoptadas; y, (iii) que sea oportuna, esto es, que las medidas idóneas ejecutadas se hayan realizado de manera acabada antes de la notificación de la imputación de cargos. Ni la subsanación adecuada ni su oportunidad exigen una reversión o reparación de efectos concretos como condición general adicional para la aplicación de la eximente sino la corrección proactiva de la conducta u omisión infractora. Para valorar la subsanación, la Dirección podrá tomar en cuenta si, considerando la acción correctora, devendría en innecesario el dictado de medidas correctivas adicionales para una adecuada prevención del riesgo de infracción.*
>
> *Esta Dirección considera pertinente precisar que el criterio adoptado se encuadra en una visión preventiva y promotora del cumplimiento que privilegia el incentivo al restablecimiento de la legalidad en salvaguarda de los derechos de los titulares de datos personales, sin perjuicio del potencial despliegue de la potestad sancionadora cuando sea necesario y aplicable conforme a derecho.*

REQUERIMIENTOS. Para permitir la exoneración de multas a empresas que sufrieron filtraciones, se han establecido tres nuevos requerimientos.

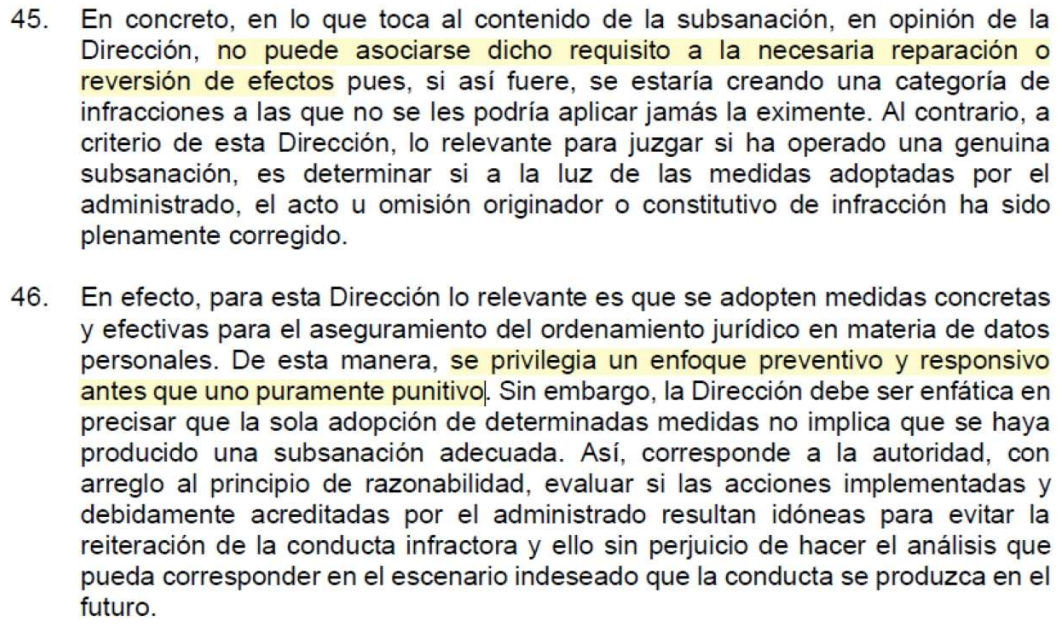
Captura de documento

Dilmar Villena, director ejecutivo de la ONG Hiperderecho, explicó que, cuando ocurren filtraciones como la de Interbank, ya no se puede subsanar el daño causado. “La información de las personas ya está expuesta, lo único que podrías hacer es retroceder en el tiempo”, señaló. Para el especialista, se trata de una situación irreversible.

En la resolución del caso Interbank, la autoridad justifica que el cambio de criterio responde a una visión preventiva de su función. Gustavo Rodríguez García, director de la ANPD desde el 16 de setiembre, habló sobre este cambio de criterios durante una reunión con empresarios realizada la segunda quincena de octubre en la Cámara de Comercio Americana del Perú (AmCham Perú).

“Las sanciones son instrumentos, no el objetivo” y “la autoridad debe dar incentivos y acompañar el desarrollo de capacidades para lograr el cumplimiento” son frases que forman parte de las diapositivas proyectadas por el funcionario, cuya trayectoria profesional se ha desarrollado principalmente en el sector privado.

Hazte Aliado/a



45. En concreto, en lo que toca al contenido de la subsanación, en opinión de la Dirección, no puede asociarse dicho requisito a la necesaria reparación o reversión de efectos pues, si así fuere, se estaría creando una categoría de infracciones a las que no se les podría aplicar jamás la eximente. Al contrario, a criterio de esta Dirección, lo relevante para juzgar si ha operado una genuina subsanación, es determinar si a la luz de las medidas adoptadas por el administrado, el acto u omisión originador o constitutivo de infracción ha sido plenamente corregido.

46. En efecto, para esta Dirección lo relevante es que se adopten medidas concretas y efectivas para el aseguramiento del ordenamiento jurídico en materia de datos personales. De esta manera, se privilegia un enfoque preventivo y responsivo antes que uno puramente punitivo. Sin embargo, la Dirección debe ser enfática en precisar que la sola adopción de determinadas medidas no implica que se haya producido una subsanación adecuada. Así, corresponde a la autoridad, con arreglo al principio de razonabilidad, evaluar si las acciones implementadas y debidamente acreditadas por el administrado resultan idóneas para evitar la reiteración de la conducta infractora y ello sin perjuicio de hacer el análisis que pueda corresponder en el escenario indeseado que la conducta se produzca en el futuro.

ENFOQUE. En la resolución del caso Interbank, la autoridad justifica que el cambio de criterio responde a una visión preventiva de su función.

Captura de documento

La abogada Marina Meira, coordinadora de Políticas Públicas de la ONG Derechos Digitales, sostuvo que, si bien incentivar una corrección rápida de daños es importante, este enfoque deja de lado las consecuencias para las personas afectadas desde una perspectiva de derechos humanos. “Entonces, los datos filtrados pueden seguir circulando y exponer a las personas titulares a fraude, discriminación y violencia”, advirtió.

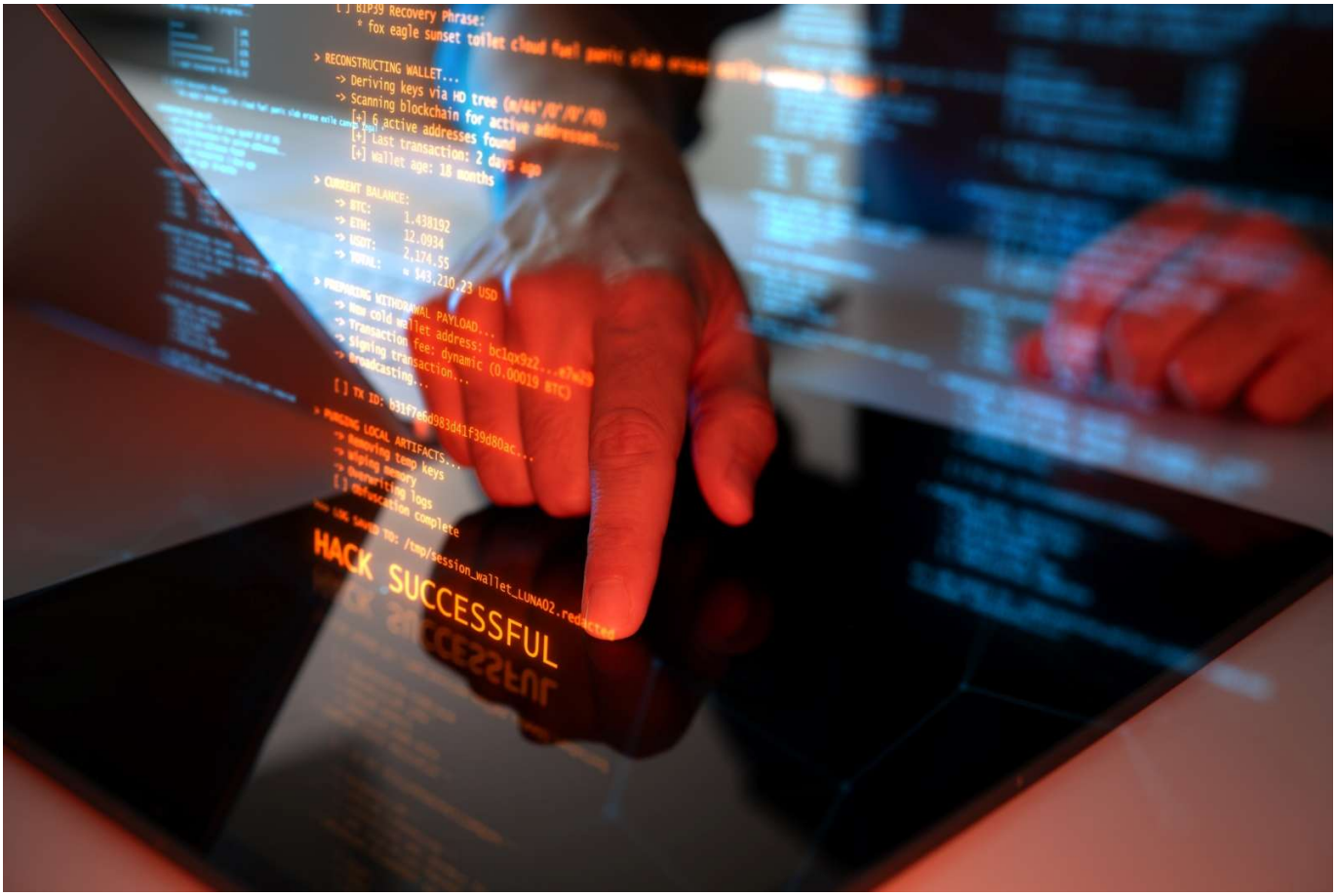
Una filtración por deficiencias en seguridad

El cambio de criterio genera cuestionamientos sobre sus posibles efectos en la protección de los datos personales. Para Dilmar Villena, el efecto de este cambio de criterio podría resultar contrario a la intención de la autoridad. Explicó que las filtraciones masivas de datos suelen ocurrir porque las entidades no han implementado medidas de seguridad adecuadas. “Pocas entidades públicas o privadas cumplen con los requisitos exigidos por la ley”, señaló.

La investigación del caso Interbank identificó precisamente deficiencias en sus sistemas de seguridad que facilitaron el robo de información. El informe detalla que el ataque comenzó cuando la computadora de un proveedor del banco fue infectada con Lumma Stealer, un programa malicioso diseñado para robar información. Una vez instalado, este se oculta en el sistema y monitorea la actividad del equipo para extraer datos.

Aunque grandes compañías han impulsado **iniciativas para frenarlo**, sigue siendo una de las herramientas más utilizadas en el mundo para obtener información personal y corporativa sensible.

Hazte Aliado/a



HACKEO. El ataque contra Interbank comenzó cuando la computadora de un proveedor del banco fue infectada con un programa malicioso.

Foto: Shutterstock

De esta manera, de acuerdo con informe de la autoridad, el atacante obtuvo una cuenta y sus credenciales de acceso a los sistemas del banco. Con esa información ingresó a seis aplicaciones de Interbank, desde las que copió y descargó grandes volúmenes de información los días 27 y 28 de setiembre de 2024.

El 12 de octubre, el banco recibió un correo electrónico del atacante, quien exigía dinero a cambio de no publicar los datos. Interbank señaló ante la autoridad que el mensaje no incluía pruebas suficientes para acreditar que la amenaza era real. Pese a esta advertencia, el banco no había detectado la extracción de datos de sus sistemas.

En la Resolución Directoral 1019, la investigación de la Autoridad Nacional de Protección de Datos Personales concluyó que el banco “no contaba con controles o medidas de seguridad que impidan accesos no autorizados e impidan abusos del servicio y/o extracción de la información correspondiente a los datos personales de sus clientes”.

Una de las principales fallas detectadas fue que Interbank permitía acceder a sus sistemas desde cualquier equipo. Según dicha investigación, restringir el ingreso a dispositivos autorizados bloquearía el acceso del atacante.

El banco tampoco contaba con alertas para detectar descargas masivas de datos de clientes, indica la resolución directoral citada. Por eso, la extracción de información realizada durante dos días pasó inadvertida. Además, no realizaba revisiones periódicas de las cuentas con acceso a su sistema, para detectar aquellas que debían ser dadas de baja.

OjoPúblico envió un cuestionario a la Autoridad Nacional de Protección de Datos Personales para conocer sus argumentos a favor del cambio de criterio, pero hasta el cierre de este informe no obtuvo respuestas. También se comunicó con Interbank sobre la multa impuesta, pero tampoco respondieron.

Resoluciones posteriores

Uno de los aspectos centrales del cambio introducido por la autoridad es el plazo que tienen las empresas para corregir sus infracciones y acceder a la exoneración de multas.

Hazte Aliado/a

Según el tercer requisito, basta con que adopten las medidas correctivas antes de recibir la notificación formal de imputación de cargos. Este periodo puede extenderse durante meses e incluso años, de acuerdo con la resolución directoral 1019.

En el caso de la filtración de datos de Interbank, la brecha de seguridad ocurrió en setiembre de 2024 y, tras iniciarse un proceso administrativo, el banco fue notificado de la imputación de cargos en diciembre de 2025. Es decir, transcurrió más de un año durante el cual el banco pudo corregir sus deficiencias de seguridad antes de recibir esa notificación.

> ***SEGÚN EL TERCER REQUISITO, BASTA CON QUE ADOPTEN LAS MEDIDAS CORRECTIVAS ANTES DE RECIBIR LA NOTIFICACIÓN FORMAL DE IMPUTACIÓN DE CARGOS.***

Dilmar Villena advirtió que, en la práctica, las empresas podrían actuar solo cuando la entidad avance con el procedimiento sancionador, mientras que las quejas de los usuarios permanecen desatendidas.

Una resolución posterior, obtenida por **OjoPúblico** y emitida seis días después de que se estableciera el nuevo criterio, muestra cómo este cambio ya comenzó a aplicarse.

El 2 de julio de 2024, una clienta de Interbank presentó una queja ante la Autoridad Nacional de Protección de Datos Personales en contra de Interbank. Señaló que el banco había enviado reiteradamente información sobre sus deudas por un crédito y una tarjeta al correo electrónico de otra persona.

La usuaria solicitó que el banco dejara de enviar su información a un tercero, pero los envíos continuaron. Tras evaluar el caso, el área de fiscalización de la autoridad recomendó imponer una multa equivalente a 24.75 Unidades Impositivas Tributarias, equivalente a S/127.462.

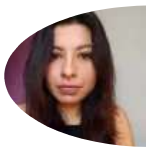
Sin embargo, la resolución de primera instancia aplicó el nuevo criterio y concluyó con eximir de responsabilidad administrativa a Interbank. El banco había señalado que realizó correcciones en su sistema para detener las notificaciones dos meses después de la denuncia de la usuaria.

“Lo que están buscando es que las empresas vean que es preferible actuar rápidamente antes de que llegue la imputación de cargos. Pero viendo cómo es el contexto peruano, posiblemente suceda que van a ignorar cualquier denuncia o pedido directo de la ciudadanía”, advirtió Dimar Villena.

Fiorella Montaño

@fiomontano

fiorella@ojo-publico.com



Relacionados

Interbank, Autoridad Nacional de Datos Personales, Datos Personales

Desafía las redes de poder

Denunciar el abuso de poder, tanto corporativo como del crimen organizado en Latinoamérica, exige una libertad editorial que solo el apoyo de nuestros lectores hace posible. Al ser nuestro **Aliado/a**, nos permites seguir exponiendo los intereses económicos que operan en las sombras y vulneran a la ciudadanía.

Hazte Aliado/a

LO MÁS LEÍDO









RECOMENDAMOS

Memorándum con EE.UU. busca acelerar permisos para minerales críticos

Memorándum de IA con EEUU busca construir más centros de datos en Perú

El millonario gasto municipal para mantener las vías de Rutas de Lima

Datos filtrados: caso Interbank deja precedente para eximir multas

Hazte Aliado/a