

PONTIFICIA UNIVERSIDAD
CATÓLICA DEL PERÚ

FACULTAD DE DERECHO



Informe Jurídico sobre la Resolución Final N° 1284-
2024/CC1

Trabajo de Suficiencia Profesional para optar el Título de Abogada
que presenta:

Ana Valentina García Reátegui

ASESOR:

Julio Baltazar Durand Carrión

Lima, 2025

Informe de Similitud

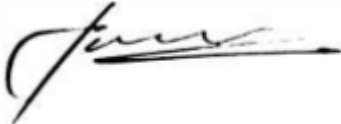
Yo, DURAND CARRION, JULIO BALTAZAR, docente de la Facultad de Derecho de la Pontificia Universidad Católica del Perú, asesor(a) del Trabajo de Suficiencia Profesional titulado "Informe Jurídico sobre la Resolución Final N° 1284-2024/CC1", del autor(a) GARCIA REATEGUI, ANA VALENTINA, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 26%. Así lo consigna el reporte de similitud emitido por el software Turnitin el 21/07/2025.

- He revisado con detalle dicho reporte y el Trabajo de Suficiencia Profesional, y no se advierten indicios de plagio.

- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lima, 21 de julio del 2025.

DURAND CARRION, JULIO BALTAZAR	
DNI: 06726360	 Firma:
ORCID: https://orcid.org/0000-0002-2926-1912	

RESUMEN

El informe es el resultado del análisis de la Resolución Final N° 1284-2014/CC1, pronunciamiento de la Comisión de Protección al Consumidor del Indecopi en materia de deber de idoneidad en la actividad del sistema bancario. En el caso materia de análisis, la señora Cecilia Arbe presenta una denuncia contra el Banco de Crédito del Perú por infracción al deber de idoneidad al no haber cumplido con adoptar las medidas de seguridad que establece la normativa sectorial permitiendo que se realice una operación no reconocida en su cuenta de ahorros.

Por lo tanto, el análisis jurídico se enfoca en responder al problema de cuáles son las garantías para brindar un servicio idóneo que involucra la protección al consumidor respecto de operaciones no reconocidas. Para responder a este planteamiento, los principales instrumentos normativos utilizados son el Código de Protección y Defensa del Consumidor, el Reglamento de Tarjetas de Crédito y Débito, y el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad. En ese sentido, mediante el análisis de los instrumentos normativos y jurisprudencia vinculada, se concluirá que la normativa sectorial prevé una protección mayor al consumidor financiero en materia de operaciones no reconocidas al establecer obligaciones cuyo incumplimiento deriva en indubitable infracción al deber de idoneidad.

Palabras clave

Consumidor financiero, deber de idoneidad, medidas de seguridad, tarjeta de débito.

ABSTRACT

The report is the result of the analysis of the Final Resolution N° 1284-2014/CC1, pronouncement of the Consumer Protection Commission of Indecopi regarding the duty of suitability in the activity of the banking system. In the case under analysis, Mrs. Cecilia Arbe file a complainant against Banco de Crédito del Perú for breach of the duty of suitability for not having complied with adopting the security measures established by the sectorial regulations, allowing an unrecognized operation to be carried out in her savings account.

Therefore, the legal analysis focuses on answering the problem of which are the guarantees to provide a suitable service involving consumer protection in respect of unrecognized operations. To respond to this approach, the main regulatory instruments used are the Code of Consumer Protection and Defense, the Credit and Debit Card Regulation, and the Regulation for the Management of Information Security and Cybersecurity. In this sense, through the analysis of the normative instruments and related jurisprudence, it will be concluded that the sectorial regulations provide a greater protection to the financial consumer in the matter of unrecognized operations by establishing obligations whose non-compliance derives in indubitable infringement to the duty of suitability.

Keywords

Financial consumer, duty of suitability, safety measures, debit card.

ÍNDICE

PRINCIPALES DATOS DEL CASO	4
I. INTRODUCCIÓN	5
1.1 Justificación de la elección de la resolución	5
1.2 Presentación del caso y del análisis	8
II. IDENTIFICACIÓN DE LOS HECHOS RELEVANTES	9
2.1 Antecedentes	9
2.2 Hechos relevantes del caso	10
III. IDENTIFICACIÓN DE LOS PRINCIPALES PROBLEMAS JURÍDICOS	12
3.1 Problema principal	12
3.2 Problemas secundarios	12
IV. POSICIÓN DEL CANDIDATO/A	13
4.1 Respuestas preliminares a los problemas principal y secundarios	13
4.2 Posición individual sobre el fallo de la resolución	14
V. ANÁLISIS DE LOS PROBLEMAS JURÍDICOS	15
VI. CONCLUSIONES	28
BIBLIOGRAFÍA	30
ANEXOS	32

PRINCIPALES DATOS DEL CASO

N° EXPEDIENTE	Expediente N° 2393-2023/PS2
ÁREA(S) DEL DERECHO SOBRE LAS CUALES VERSA EL CONTENIDO DEL PRESENTE CASO	Derecho Administrativo / Protección al Consumidor
IDENTIFICACIÓN DE LAS RESOLUCIONES Y SENTENCIAS MÁS IMPORTANTES	-
DEMANDANTE/DENUNCIANTE	Cecilia Ximena Arbe Braga
DEMANDADO/DENUNCIADO	Banco de Crédito del Perú S.A.
INSTANCIA ADMINISTRATIVA O JURISDICCIONAL	Administrativa
TERCEROS	-
OTROS	-

I. INTRODUCCIÓN

1.1 Justificación de la elección de la resolución

El presente informe abordará el análisis de la Resolución Final N° 1284-2024/CC1, pronunciamiento de la Comisión de Protección al Consumidor N° 01 sobre recurso de apelación formulado por la señora Cecilia Arbe contra la resolución de primera instancia que resolvió archivar el procedimiento iniciado contra el Banco de Crédito del Perú por presunta infracción de los artículos 1 inciso c), 18 y 19 del Código de Protección y Defensa del Consumidor.

En el contexto actual, es considerablemente alto el número de denuncias en materia de protección al consumidor contra entidades bancarias por motivo de operaciones no reconocidas. El caso de la señora Arbe no es una excepción en tanto versa sobre una operación no reconocida por aplicación deficiente de factores de autenticación reforzada reglamentarios por parte de la entidad bancaria.

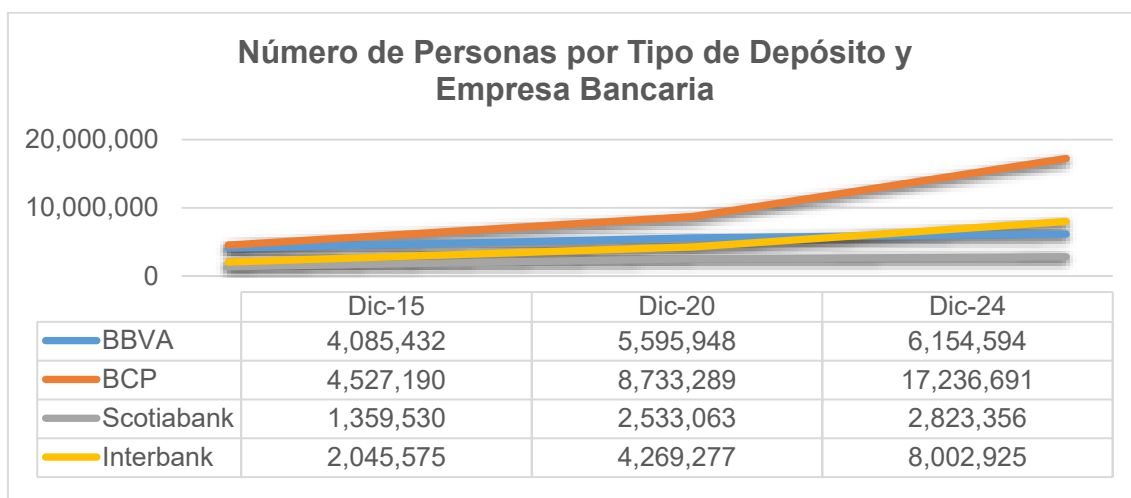
En ese sentido, dado que actualmente existe un fenómeno de bancarización de toda la población y un crecimiento exponencial del mercado financiero y las transacciones bancarias y financieras que se fomentan, sí amerita realizarse el análisis de la protección al consumidor en materia de servicios bancarios que, incluso siendo seriamente regulado, concentra el 90% de sanciones por parte del Indecopi en operaciones no reconocidas (Indecopi, 16 de abril de 2025).

Tras la revisión del Portal SBS sobre el Sistema Financiero¹, considero que la materia sí amerita su amplia regulación en tanto el número de depositantes desde diciembre 2015 a diciembre de 2020 creció en 73.29%. Siendo que, de la última fecha mencionada a diciembre de 2024, creció en 52.85%.

Asimismo, si evaluamos el crecimiento de las entidades bancarias/financieras más importantes del Perú, se puede apreciar que la cantidad de personas que

¹ Información recuperada del Portal Web de la SBS.

realizan depósitos de tipo ahorro mínimamente se duplicaron, conforme se aprecia en el gráfico a continuación:



Elaboración propia con información obtenida del Portal SBS

Sin perjuicio de ello, un aspecto que resulta crucial evaluar consiste en el posicionamiento de determinadas entidades bancarias a lo largo del tiempo. Tanto BBVA (antes Banco Continental), Banco de Crédito del Perú, Scotiabank Perú e Interbank ocupaban el 82.88% del mercado en diciembre de 2015. Posteriormente, en diciembre de 2024, la distribución del mercado no ha variado significativamente en tanto apreciamos que ahora las empresas consolidan el 82.93% del mercado, conforme se aprecia en el gráfico a continuación:



Elaboración propia con información obtenida del Portal SBS

El posicionamiento y la concentración de consumidores en cuatro entidades financieras es uno de los fundamentos principales para establecer regulación

numerosa y detallada sobre las obligaciones que deben cumplir. Considerando también que, la formación de un oligopolio no genera incentivos de mejora o innovación en pro de los consumidores para estas empresas, puesto que, dentro de todo, es altamente probable que siempre una de ellas sea elegida por estos.

El rol de la autoridad en materia financiera ha sido fundamental para dictar normas que establezcan obligaciones para los proveedores sobre seguridad de los consumidores financieros. Al respecto, mediante Resolución SBS N° 6523-2013 – Reglamento de Tarjetas de Crédito y Débito emitido el 30 de octubre de 2013, la autoridad ha buscado establecer claramente, entre otros, cuáles son las obligaciones aplicables a las empresas de banca múltiple que han sido autorizadas a administrar las tarjetas de crédito y débito.

Esto ha resultado determinante en tanto el número de tarjetas ha fluctuado en los últimos 10 años, con tendencia a crecimiento, bien sea mediante la contratación de tarjetas de débito como de tarjetas de crédito en las entidades bancarias con mayor posicionamiento en el mercado.

De esa forma, resulta necesario identificar cuáles son las garantías para brindar un servicio idóneo que involucra la protección al consumidor financiero en materia de operaciones no reconocidas y, entre ellas, cuáles son las obligaciones a cumplir por las entidades bancarias que exige la normativa sectorial en la materia. Siendo así, se buscará conocer cómo se determina que un producto o servicio financiero brindado ha sido idóneo al presentarse una operación no reconocida.

Todo ello, con la finalidad de evaluar cual fue el criterio de la Comisión para se cometió infracción contra el deber de idoneidad, contrario al criterio de primera instancia que debido al rompimiento del nexo causal por imprudencia de la consumidora determinó el archivo del procedimiento. Por tanto, la relevancia de la Resolución elegida consiste en que permitirá evaluar aspectos cruciales vinculados al deber de idoneidad en protección del consumidor con relación a los servicios bancarios y las obligaciones de los proveedores de estos servicios.

1.2 Presentación del caso y del análisis

El caso versa sobre el fraude informático del cual fue víctima la señora Cecilia Arbe tras el robo de sus pertenencias. Ante ello, formuló dos reclamos ante el Banco de Crédito para solicitar el extorno del monto usurpado de su cuenta de ahorros. Sin embargo, el Banco negó su solicitud y la señora Arbe presenta denuncia ante el Órgano de Procedimientos Sumarísimos (en adelante, “el OPS”).

En primera instancia, el OPS resuelve declarar infundada la denuncia señalando que se habría roto el nexo causal por imprudencia de la consumidora. Así, la consumidora formula recurso de apelación y la Comisión de Protección al Consumidor N° 01 resuelve revocar la resolución de primera instancia y reformándola, declara fundada la denuncia.

Esto genera la pregunta sobre cuáles son las garantías que establece el ordenamiento peruano ante operaciones no reconocidas para que las entidades bancarias brinden un servicio financiero idóneo al consumidor. Así como, de forma secundaria, cuáles son las medidas de seguridad que exige la normativa sectorial y cuándo se considera que un servicio es idóneo respecto a operaciones no reconocidas. Todo ello evaluando cuál es el criterio de la Comisión para considerar si se cometió infracción contra el deber de idoneidad.

Al respecto, de forma breve, considero que el sistema de protección al consumidor se ha encargado de establecer garantías para los consumidores que se sustentan en el artículo 65 de la Constitución Política del Perú, y la Superintendencia de Banca y Seguros, a través de su normativa sectorial, también se ha encargado de establecer obligaciones claras para las entidades que proveen servicios bancarios y financieros al consumidor.

Sin perjuicio de ello, el rol del Indecopi se vuelve imprescindible para evaluar la casuística que atraviesan los consumidores, así como para verificar la aplicación, en marco de sus competencias reconocidas, las normas aplicables a la materia. En ese sentido, considero que la Resolución a evaluar en el informe jurídico es

especialmente relevante porque aborda el cumplimiento de medidas de seguridad como cuestión primordial y del deber de idoneidad sin valorar si la conducta de la consumidora fue imprudente o no.

Para realizar el presente informe, se ha revisado doctrina nacional vinculada a la materia y legislación, tanto el Código de Consumo, así como resoluciones de la SBS; pero el análisis comprende principalmente la revisión de resoluciones emitidas por la Sala Especializada en Protección al Consumidor sobre la materia.

II. IDENTIFICACIÓN DE LOS HECHOS RELEVANTES

2.1 Antecedentes

El 12 de octubre de 2022 la señora Cecilia Arbe contrata una cuenta de ahorros en el Banco de Crédito asociada a una Tarjeta de Débito. Posteriormente, el 14 de julio de 2023 la señora Arbe es víctima de robo de sus pertenencias que deriva en un fraude informático que origina una operación no reconocida con cargo en su cuenta de ahorros:

BANCO RECEPTOR DE LA TRANSFERENCIA	FECHA DE LA TRANSFERENCIA	MONTO TRANSFERIDO
Scotiabank Perú S.A.A.	14 de julio de 2023	S/ 5,204.80

Ante ello, la señora Arbe procede a solicitar el bloqueo de su tarjeta y formula un reclamo ante el referido Banco solicitando la devolución del importe, y el 17 de julio de 2023 Banco responde que la devolución no sería posible porque la operación habría sido realizada siguiendo los parámetros de seguridad. En la misma fecha, la señora Arbe formula nuevamente un reclamo ante el Banco, pero el 26 de julio la entidad bancaria responde denegando nuevamente la solicitud de devolución de la señora Arbe.

2.2 Hechos relevantes del caso

a) Presentación de la denuncia

El **04 de setiembre de 2023** la señora Arbe formula denuncia contra el Banco imputando las siguientes conductas: (i) infracción al deber de idoneidad por no adoptar oportunamente las medidas de seguridad necesarias para impedir una operación no reconocida en su cuenta de ahorro, y (ii) infracción al deber de información por no comunicar oportuna y repetidamente en el mercado las medidas de seguridad y prevención para evitar fraudes informáticos.

b) Admisión a trámite de la denuncia

Mediante la **Resolución N° 01 de fecha 13 de setiembre de 2023** el OPS N° 02 inicia un procedimiento administrativo sancionador imputando el siguiente cargo: presunta infracción al deber de protección de los intereses económicos y al deber de idoneidad tipificados en los artículos 1 inciso c), 18 y 19 del Código de Consumo.

Asimismo, el OPS requirió la presentación de documentación vinculada al procedimientos y mecanismos de seguridad para autorizar operaciones, datos sobre la operación cuestionada, reporte de sistema con el registro de movimientos de la denunciante, copia del contrato, entre otros.

Posteriormente, el **19 de octubre de 2023** el Banco contesta la denuncia de la señora Arbe indicando que la operación se dio válidamente antes de que la denunciante solicitara el bloqueo de su tarjeta y que corresponde la aplicación del artículo 23 de la Resolución SBS N° 6523-2013 en tanto la conducta de la denunciante fue negligente al no reportar el hecho ni solicitar el bloqueo de su tarjeta.

c) Pronunciamiento del Órgano de Procedimientos Sumarísimos

Mediante **Resolución Final N° 1881-2023/PS2 de fecha 26 de octubre de 2023** el OPS indica que el Banco no cumplió con el circuito de autenticación reforzada, sin embargo, corresponde la aplicación del artículo 104 del Código de Consumo que dispone la exoneración de responsabilidad por imprudencia del consumidor en tanto el comportamiento negligente de la denunciante habría generado el rompimiento del nexo causal. En ese sentido, el OPS resuelve archivar el procedimiento administrativo sancionador.

d) Recurso de apelación presentado por la denunciante

El **23 de noviembre de 2023** la señora Arbe formula recurso de apelación contra la Resolución señalando que el Banco no cumplió con el circuito de autenticación reforzada ni adoptó las medidas de seguridad idóneas para monitorear una operación fuera de su patrón habitual de consumo.

Mediante **Resolución N° 02 de fecha 10 de abril de 2024**, la Secretaria Técnica e la Comisión efectúa requerimiento de información y el **17 de abril de 2024** el Banco atiende el requerimiento de información parcialmente aduciendo que la Comisión no tiene competencia para verificar el cumplimiento de medidas de ciberseguridad.

e) Pronunciamiento de la Comisión en segunda instancia

Posteriormente, mediante **Resolución Final N° 1284-2024/CC1 de fecha 05 de junio de 2024** la CC1 se pronuncia revocando la Resolución de primera instancia y declara fundada la denuncia por infracción de los artículos 1.c, 18 y 19 del Código de Protección y Defensa del Consumidor, ordena la restitución del monto de la operación no reconocida y sanciona al Banco con una multa de 3.78 UIT. La Comisión sustenta su decisión indicando que el Banco no cumplió con el circuito de autenticación reforzada por lo que corresponde sancionarlo por vulneración al principio de idoneidad.

III. IDENTIFICACIÓN DE LOS PRINCIPALES PROBLEMAS JURÍDICOS

3.1 Problema principal

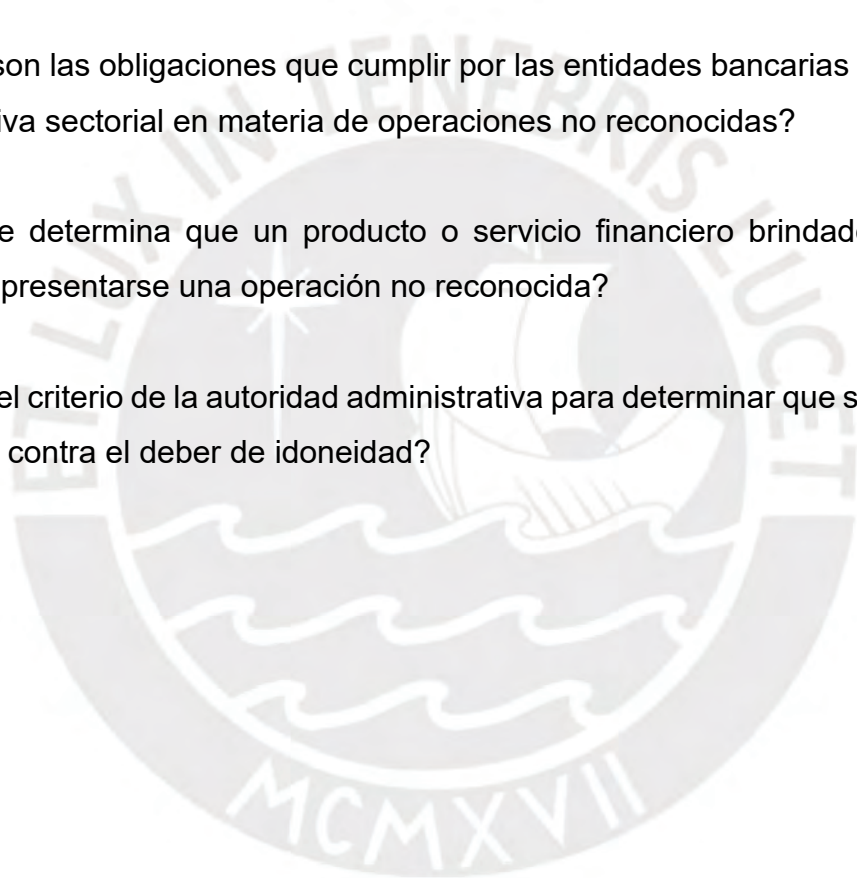
¿Cuáles son las garantías para brindar un servicio idóneo que involucra la protección al consumidor respecto de operaciones no reconocidas?

3.2 Problemas secundarios

¿Cuáles son las obligaciones que cumplir por las entidades bancarias que exige la normativa sectorial en materia de operaciones no reconocidas?

¿Cómo se determina que un producto o servicio financiero brindado ha sido idóneo al presentarse una operación no reconocida?

¿Cuál es el criterio de la autoridad administrativa para determinar que se cometió infracción contra el deber de idoneidad?



IV. POSICIÓN DEL CANDIDATO/A

4.1 Respuestas preliminares a los problemas principal y secundarios

Respecto al problema principal sobre cuáles son las garantías para brindar un servicio idóneo que involucra la protección al consumidor respecto de operaciones no reconocidas, nuestra norma constitucional prevé un sistema garantista en favor del consumidor, conforme al artículo 65. En ese mismo sentido, el Código de Consumo establece obligaciones para los proveedores, y, en el caso de proveedores de servicios bancarios y financieros, la normativa sectorial se ha encargado de establecer obligaciones específicas y técnicas para salvaguardar las operaciones realizadas por los consumidores.

Respecto al problema secundario sobre cuáles son las obligaciones que cumplir por las entidades bancarias que exige la normativa sectorial en materia de operaciones no reconocidas, la normativa sectorial establece medidas que deben adoptar los proveedores de servicios bancarios y financieros para frente a operaciones con tarjetas de los consumidores a través de los artículos 17 y 22 del Reglamento de Tarjetas de Crédito y Débito.

Respecto al problema secundario sobre cómo se determina que un producto o servicio brindado cumple con el deber de idoneidad al presentarse una operación no reconocida, es crucial determinarlo según las implicancias de los artículos 18 y 19 del Código. Al respecto, considero que el Banco incurre en infracción al deber de idoneidad al incumplir con el circuito de autenticación reforzada.

Respecto al problema secundario sobre cuál es el criterio de la autoridad administrativa para considerar que se cometió infracción contra el deber de idoneidad, la Comisión se decanta por sancionar al proveedor por no cumplir con el último paso del circuito de autenticación reforzada indicando que los medios probatorios presentados no pueden acreditar el envío y recepción de la notificación de la operación. Sin perjuicio de ello, la Comisión sigue el criterio de que, al tratarse de una sola operación, no se puede acreditar que el Banco haya

cumplido con las medidas de seguridad sobre el sistema de monitoreo, así como no aplica los artículos 22 y 23 del Reglamento de Tarjetas.

4.2 Posición individual sobre el fallo de la resolución

Estoy parcialmente de acuerdo con la Resolución de la Comisión de Protección al Consumidor N° 01. En mi opinión, el fallo de la Comisión que resuelve infracción al deber de idoneidad debido al incumplimiento del circuito de autenticación reforzada es correcto, sin embargo, primero se debió evaluar si la operación se alineaba dentro del comportamiento habitual de la consumidora o no. En ese supuesto, la transacción debitada de la cuenta de ahorros de la consumidora no se alineaba con su patrón de consumo y, por ende, el Banco no cumple con el deber de monitoreo de las operaciones de los usuarios.

Asimismo, la autoridad debió aplicar los artículos 22 y 23 del Reglamento de Tarjetas. También, considero que la Comisión pudo pronunciarse sobre la importancia de que los órganos administrativos se encarguen de evaluar primero que los proveedores cumplan con las obligaciones que establece la normativa antes que evaluar el comportamiento del consumidor, como erróneamente realizó el OPS al restringirse a evaluar la conducta de la denunciante para emitir su resolución.

V. ANÁLISIS DE LOS PROBLEMAS JURÍDICOS

Problema secundario 1: ¿Cuáles son las obligaciones que cumplir por las entidades bancarias que exige la normativa sectorial en materia de operaciones no reconocidas?

Acorde con el Artículo 87 de la Constitución, la designación de competencias a la SBS se desprende de la finalidad estatal de fomentar y proteger el ahorro de los ciudadanos. Las competencias que se asignan a la autoridad en materia bancaria permiten que regule los límites y las obligaciones de las entidades financieras. Para ello, la norma constitucional otorga autonomía funcional, presupuestal y administrativa que le permite cumplir con supervisar el debido funcionamiento del sistema financiero y bancario.

Por lo que, dentro de las funciones que establece la normativa nacional para la SBS, se puede identificar que la autoridad debe cumplir con regular y supervisar a todas las empresas dentro del mercado financiero y de seguros, sin perjuicio de aquellas que puedan estar vinculadas a la materia por realizar operaciones indirectamente vinculadas o que resulten complementarias a aquellas empresas que sí resultan claramente bancarias/financieras.

Así, la SBS se encarga de autorizar funcionamiento, velar por el cumplimiento de las normas, interpretar en vía administrativa las normas aplicables, dictar normativa específica, realizar inspecciones inopinadas y, en general, realizar acciones vinculadas al sector financiero que permitan salvaguardar los intereses de los ciudadanos.

Entonces, resulta claro que la SBS es la autoridad que se encarga de vigilar el correcto funcionamiento de las entidades del sector financiero e, indirectamente, poder salvaguardar derechos e intereses. También resulta evidente que la autoridad cumple un rol en la protección de los consumidores de manera indirecta mediante el impulso de la educación financiera y la posibilidad que brinda de presentar denuncias si una entidad financiera incumple con la normativa sectorial.

En ese marco y para efectos del presente trabajo, corresponde mencionar cuál es el rol del Indecopi en materia bancaria. Para ello, es importante remitirnos brevemente al cuestionamiento sobre la competencia entre la SBS y el Indecopi que, en años anteriores, fue materia de controversia y que, en la actualidad, ambas autoridades se han encargado de establecer claramente sus competencias específicas.

Por su parte, el Indecopi como autoridad clave y competente en salvaguardar los derechos de los consumidores, se encarga de velar por estos en lo relacionado a una relación de consumo dentro del territorio nacional. Como parte de ello, el Código delimita su ámbito de aplicación para todos los consumidores que puedan verse involucrados directa o indirectamente en una relación de consumo o en operaciones a título gratuito que busquen fomentar el consumo (Artículo III). Ello habilita a que pueden presentar denuncias si el proveedor no cumple con el sistema de garantías que corresponde.

Por tanto, mientras que el Indecopi protege el bien jurídico de tutela del consumidor, la SBS tutela el bien jurídico que comprende el debido funcionamiento del sistema financiero. Así, la SBS establece una protección macroeconómica del mercado, mientras que el Indecopi una protección microeconómica.

En ese mismo sentido, mediante el fundamento 42 de la Resolución N° 1332-2018/SPC-INDECOPI, la Sala Especializada en Protección al Consumidor menciona lo siguiente:

“42. Por otro lado, esta Sala hace notar que, de los actuados, no se advierte vulneración al principio non bis in ídem, en la medida que la SBS y el Indecopi tutelan bienes jurídicos distintos, siendo que la primera entidad tutela fundamentalmente el funcionamiento y operatividad del sistema financiero, y el Indecopi los derechos de los consumidores con relación a los productos o servicios que adquieren, utilizan o disfrutan”.

Así, como destaca la Sala, no cabe alegar vulneración al principio non bis in ídem en tanto el fundamento para la aplicación de las competencias de las referidas autoridades administrativas no es el mismo.

En la Resolución objeto de análisis, el proveedor denunciado cuestiona la competencia del Indecopi para emitir pronunciamientos respecto a los aspectos técnicos u obligaciones derivadas del Reglamento de Ciberseguridad e indica que la entidad competencia sería la SBS. Esto se evidencia en el escrito de fecha 17 de abril de 2024 parte de expediente del caso, que menciona lo siguiente: “la autoridad competente para indagar aspectos técnicos relacionados al Reglamento de Ciberseguridad y verificar el cumplimiento de este es la Superintendencia de Banca, Seguros y AFP, en su condición de entidad supervisora de las empresas del sistema financiero y **no** el Indecopi (...).

Discrepo totalmente de esta postura, puesto que, tras la interpretación de la regulación nacional y el posterior desarrollo jurisprudencial, el Indecopi no solo posee competencia, sino que está obligado a pronunciarse sobre la aplicación de la normativa sectorial destinada a la protección del consumidor.

Al respecto, en el fundamento 23 de la Resolución N° 1284-2024/CC1, se rescata que: “El artículo 19 del Reglamento de Sanciones señala que será la SBS la entidad competente para conocer los incumplimientos de las disposiciones que rigen a las empresas supervisadas en su relación directa con el cliente cuando constituyan un patrón de conducta, (...); asimismo, establece que los casos individuales que contengan materia amparada por las normas de protección al consumidor serán derivados al Indecopi.”

Entonces, la SBS será la entidad competente para pronunciarse sobre las infracciones de entidades financieras a las obligaciones respecto de los consumidores siempre y cuando se trate de un patrón de conducta, no en casos individuales.

Asimismo, en el fundamento 27 de la Resolución N° 1284-2024/CC1, la Comisión indica que el Indecopi está obligado a aplicar la normativa sectorial y constatar si se ha cumplido con ella o no, para poder brindar atención a la denuncia formulada por la consumidora, considerando que esta normativa involucra las obligaciones del proveedor respecto de la relación de consumo. Sin perjuicio de que, siempre puede solicitar a la SBS que emita un informe técnico respecto a la normativa para que el pronunciamiento del Indecopi sea acorde a derecho.

En ese sentido, si el Indecopi no tuviera la competencia para pronunciarse respecto al cumplimiento de la normativa técnica y específica, y de las obligaciones que de esta se desprenden, no podría evaluar correctamente si la conducta imputada al proveedor incurre en infracción o no en perjuicio de los consumidores.

Como antesala, es importante precisar que las transacciones financieras pueden ser realizadas de diferentes formas. Siendo que, en la actualidad, estas transacciones cuentan con la facilidad de efectuarse a través de canales digitales. La innovación que conlleva el poder utilizar este medio, también implica el establecer y actualizar constantemente los mecanismos que garantizan que el ahorro de los consumidores no se encuentra bajo riesgo constante.

En ese marco, en el artículo 17 del Reglamento de Tarjetas establece como obligación a las empresas que adopten medidas de seguridad como sistemas de monitoreo y realización de operaciones por canal digital, así como de identificación de patrones de fraude. Adicionalmente, se complementa con el artículo 22 que establece obligaciones para el seguimiento de operaciones que pueden corresponder a patrones de fraude.

Entonces, los artículos 17 y 22 establecen obligaciones para que una entidad bancaria brinde seguridad sobre las operaciones que se realizan a través de canales digitales. Asimismo, el artículo 23 del Reglamento establece que la entidad bancaria será responsable de probar que se cumplió con las obligaciones de autenticación y registro de las operaciones. Además, prevé los escenarios en

los que la entidad será responsable por las pérdidas que puedan sufrir los consumidores.

La denuncia que analiza la Resolución, objeto del presente informe, surge a partir de una operación no reconocida por la consumidora que consistió en una transferencia del monto de S/. 5,204.80 (cinco mil doscientos cuatro soles y 80/100) de su cuenta de ahorros a una cuenta de terceros, que no coincide con su historial de consumos y que habría sido autorizada por la autoridad bancaria incluso ante el incumplimiento de medidas de seguridad conforme a lo alegado por la consumidora denunciante.

Cuando se habla de obligaciones, adicionalmente a la exigencia de las medidas de seguridad referidas al sistema de monitoreo de las operaciones, corresponde la aplicación del Reglamento de Ciberseguridad para operaciones realizadas por canal digital. Este Reglamento plantea conceptos técnicos cuya aplicación resulta en un proceso de autenticación reforzada que, en teoría, solo permitirá que los usuarios titulares de las cuentas puedan acceder a sus aplicativos y/o realizar operaciones en sus cuentas bancarias.

Así, los artículos 2 inciso j), 18 y 19 del Reglamento de Ciberseguridad se vinculan al proceso de autenticación reforzada. Principalmente, el artículo 19, determina que la autenticación reforzada de las operaciones consiste en tres pasos: (1) Combinación de factores de autenticación, (2) Generación de un código de autenticación a través de métodos criptográficos, y (3) La notificación exitosa de los datos de la operación al usuario.

A consideración del Boletín Semanal SBS Informa N° 24 (2022), una de las acciones que pueden suscitar operaciones fraudulentas son las operaciones de transferencia de fondos hacia cuentas de terceros. En concordancia con ello, la denuncia suscita por una transferencia de fondos en la cual, de los hechos del caso, la entidad bancaria solo cumplió con acreditar hasta el segundo requisito del circuito de autenticación referido a la generación de un código de autenticación, indicando que este consiste en el clave token.

Sin embargo, respecto al primer requisito que consiste en la combinación de factores autenticación, el BCP se limitó a indicar que el Indecopi no es la autoridad competente para evaluar si se cumplieron las medidas de seguridad; cuando, como se ha mencionado antes, no cabe duda de que sí cuenta con competencia para pronunciarse sobre ello.

Asimismo, si bien la entidad bancaria cumple con remitir una constancia sobre la notificación de la operación a la denunciante, no cumple con probar que la notificación fue efectivamente recibida. Es importante establecer que la entidad bancaria tiene la carga de la prueba en el procedimiento y que, incluso si se trata de un estándar probatorio objetivamente alto (el acreditar que el consumidor recibe una constancia), en su calidad de proveedor de un servicio con particularidades técnicas e innovadoras, tiene los medios para acreditar lo solicitado.

De acuerdo con lo señalado previamente vinculado a la normativa sectorial, en específico, a los artículos 17 y 22 del Reglamento de Tarjetas, las entidades cuentan con obligaciones claras y específicas en lo vinculado a las operaciones que se realizan por canal digital. Concretamente, tienen la obligación de implementar mecanismos de seguridad y seguimiento de estas operaciones para evitar que ocurran fraudes informáticos.

De la mano con ello, el Reglamento de Ciberseguridad plantea un método de autenticación reforzada que debe ser implementado por las entidades bancarias y que, de no cumplir con los tres pasos que establece, incurre en infracción al deber de idoneidad en la prestación del servicio financiero.

Por lo que, la aplicación conjunta de las normas que desarrolla la autoridad administrativa respecto a seguridad de este tipo de operaciones, en materia del procedimiento accionado por la denunciante, determina que es el proveedor el encargado de probar que cumplió con las obligaciones de la normativa sectorial y el Código de Consumo.

Resulta evidente entonces que las obligaciones a cumplir por las entidades bancarias que exige la normativa sectorial han sido recogidas expresamente tanto en el Reglamento de Tarjetas de Crédito y Débito, y en el Reglamento de Ciberseguridad, otorgando mayor protección al consumidor.

Entonces, a manera de conclusión parcial, las obligaciones consisten en el sistema de monitoreo, implementación de medidas de seguridad, así como en el fortalecimiento y cumplimiento del circuito de autenticación reforzada de las operaciones por canal digital.

Por lo que, la imputación de responsabilidad por parte de la Comisión en segunda instancia a la entidad bancaria es correcta por haber permitido se realice una operación sin haberse cumplido con las medidas de ciberseguridad.

Problema secundario 2: ¿Cómo se determina que un producto o servicio financiero brindado ha sido idóneo al presentarse una operación no reconocida?

Para determinar que un producto financiero ha sido debidamente brindado conforme a los parámetros de idoneidad, es importante definir que el deber de idoneidad consiste en la obligación del proveedor de brindar un producto o servicio que cumpla con características, naturaleza, condiciones u otros que a los que se encuentra obligado por norma, ha prometido o se entienden incluidos por usos del mercado.

Al respecto, el artículo 18 del Código de Consumo refiere que la idoneidad consiste, en simple, en la concordancia entre lo que el consumidor espera recibir y lo que recibe. Esta definición se complementa en entender que el producto o servicio debe responder a su naturaleza o finalidad en función a lo regulado por la normativa, lo que ha ofrecido el proveedor textualmente y lo que se espera según la finalidad de este producto o servicio, siempre atendiendo al caso en concreto.

Por su parte, el artículo 19 del Código de Consumo establece que el proveedor será responsable por la idoneidad de los productos y servicios que pone en

circulación en el mercado, pero no limitándose a ello, sino también a todo lo vinculado que bien podría consistir en la autenticidad de la marca o la publicidad comercial que ha transmitido sobre estos productos o servicios, entre otros.

Por lo que, no se trata solo de un deber de obligatorio cumplimiento, sino que también incorpora un mecanismo de tutela para los consumidores que identifiquen que el producto o servicio recibido no cumple con las garantías que recoge la norma. Así lo recoge el fundamento 29 de la Resolución N° 2221-2012/SC2-Indecopi de fecha 23 de setiembre de 2012, cuando indica que no se trata solo de un mecanismo de tutela de derechos, sino también de un mecanismo de solución que debe otorgar el proveedor si no cumple con el deber de idoneidad.

De esta forma, este deber se puede entender desde tres perspectivas muy importantes para el consumidor: (i) obliga a los proveedores a prestar un servicio o brindar un producto de acuerdo con el sistema de garantías, (ii) es un mecanismo para tutelar sus derechos e intereses, y (iii) funciona como mecanismo de solución.

Así, de acuerdo con el artículo 20 del Código de Consumo, “las garantías son las características, condiciones o términos con los que cuenta el producto o servicio.” En primer lugar, de acuerdo con el inciso a) del citado artículo, la garantía legal consiste en que, “por mandato de la ley o de las regulaciones vigentes no se permite la comercialización de un producto o la prestación de un servicio sin cumplir con la referida garantía.”

Así, una garantía legal será el parámetro mínimo e indispensable de cumplimiento obligatorio para el proveedor. Es oponible a todos los consumidores y su sustento está en la normativa. No es posible que el proveedor desconozca o refute una garantía legal, en tanto se presume su existencia incluso cuando no han sido señaladas en el contrato de consumo o en los términos expresados por el proveedor.

En segundo lugar, conforme con el inciso b) del artículo señalado, una garantía explícita consiste en la obligación que surge por los “términos y condiciones expresamente ofrecidos por el proveedor al consumidor en el contrato, (...) o cualquier otro medio por el que se pruebe específicamente lo ofrecido al consumidor.”

Dentro del sistema de garantías, la garantía expresa se compone de acuerdo con lo ofrecido expresamente por el proveedor sin que ello se trate de una obligación normativa. De acuerdo con esta garantía, a través del cualquier medio escrito, como el contrato de consumo y/o los términos y condiciones del producto o servicio, el proveedor se obliga a cumplir con todas aquellas condiciones ofrecidas.

En tercer lugar, en el inciso c) del referido artículo, se hace referencia a una garantía como implícita cuando: “ante el silencio del proveedor o del contrato, (...) el producto o servicio cumplen con los fines y usos previsibles para los que han sido adquiridos por el consumidor considerando, entre otros aspectos, los usos y costumbres del mercado.”

Este tipo de garantía no puede desplazar a ninguna de las otras garantías mencionadas, sin embargo, son especialmente importantes si atendemos a los fines y usos previsibles, especialmente si hablamos de un servicio financiero.

En ese sentido, la garantía implícita dependerá de lo que un consumidor razonable válidamente entiende que debe proveer la entidad bancaria en atención a la naturaleza de sus productos y servicios financieros ofrecidos. Así, como parte del cumplimiento de esta garantía, las entidades bancarias buscan consolidar la confianza a los usuarios.

Habiendo mencionado ello, cuando hablamos del cumplimiento del deber de idoneidad, nos remitimos a las garantías legales expresadas como medidas de seguridad que establece la normativa sectorial, en el presente caso, principalmente los artículos 17 y 22 del Reglamento de Tarjetas. Asimismo, las

garantías expresas que se encuentran previstas en los contratos suscritos por los usuarios/consumidores de los productos y servicios que ofrecen los bancos.

Sin perjuicio de ello, también hablamos de la confianza como garantía implícita que, si bien no es obligatoria, es un estándar que las entidades bancarias se comprometen a cumplir en la relación de consumo con los usuarios de sus productos y/o servicios.

Asimismo, cabe resaltar que, siempre corresponderá evaluar el cumplimiento de las obligaciones del proveedor de acuerdo con el Código de Consumo y a la normativa sectorial que corresponda. Tras haberse evaluado ello y habiendo determinado que se cumplió efectivamente con estas obligaciones, se podrá evaluar si fue el comportamiento del consumidor financiero lo que determinó que se realice la conducta denunciada. Por ejemplo, la imprudencia del consumidor.

En atención a este sistema de garantías, y como se analizará en el acápite siguiente, la exoneración de responsabilidad al proveedor no procede habiendo evaluado solamente la conducta del consumidor financiero; sino que, la autoridad administrativa primero deberá corroborar que la conducta del proveedor se realizó en cumplimiento de las garantías y obligaciones que le competen, para evaluar posteriormente si el supuesto de hecho encaja en las conductas tipificadas en el artículo 104 del Código de Consumo que regula la exoneración de responsabilidad administrativa.

En conclusión, se determina que un producto o servicio financiero cumple con el parámetro de idoneidad cuando ha sido brindado o prestado de acuerdo con las garantías establecidas tanto en la normativa como las ofrecidas directamente por el proveedor, así como aquellas que son esperables para el consumidor en atención a los fines y usos previsibles.

Problema secundario 3: ¿Cuál es el criterio de la Comisión para considerar que se cometió infracción contra el deber de idoneidad?

Previo al análisis del criterio de la Comisión para resolver que la entidad bancaria cometió una infracción contra el deber de idoneidad en segunda instancia, dentro del procedimiento administrativo, en primera instancia el OPS había resuelto declarar el archivo de la denuncia bajo la innecesaria aplicación del artículo 104 del Código de Consumo.

Al respecto, el OPS determinó que la denunciante incurre en una conducta imprudente al no solicitar el bloqueo de su tarjeta ni haber informado del robo dentro de un plazo razonable, incluso sin haber estado impedida de hacerlo. Por lo que, para la autoridad de primera instancia los hechos generarían el rompimiento del nexo causal y la exoneración de responsabilidad del denunciado.

La autoridad de primera instancia consideró que, a pesar de que la entidad financiera no pudo acreditar el cumplimiento del mecanismo de autenticación, es decir, no pudo acreditar que había cumplido con las obligaciones establecidas por normativa sectorial; le correspondía exonerarla de responsabilidad.

Parte del razonamiento de primera instancia se basa en el fundamento 29 de la Resolución Final N° 1881-2023/PS2, en el que se indica que:

“(…) el artículo 104° del Código dispone que el proveedor se exonera de responsabilidad si se demuestra la imprudencia del consumidor afectado. Así, si bien el artículo 23° del Reglamento obliga a las entidades financieras a demostrar la validez de una operación no reconocida por el titular del medio de pago, no es menos cierto que el Código es una norma de mayor jerarquía, que prevé expresamente la liberación de responsabilidad administrativa ante determinadas causales, siendo una de ellas la que se ha presentado en este caso.”

El criterio de primera instancia consiste en aplicar el Código como norma de mayor jerarquía desconociendo la protección al consumidor que otorga la normativa sectorial y, por ende, determinar la exoneración de responsabilidad incluso si el proveedor ha incumplido con sus obligaciones.

El razonamiento de la primera instancia es equivocado en tanto el mismo Código de Consumo, en el Inciso 6 del artículo V de su Título Preliminar, se sujeta al principio de protección mínima que dictamina lo siguiente: “El presente Código contiene las normas de mínima protección a los consumidores y no impide que las normas sectoriales puedan dispensar un nivel de protección mayor.”

Esto implica que, si bien el Código es una norma de mayor jerarquía, no impide que la normativa sectorial vinculada sea observada por la autoridad administrativa para determinar si el proveedor incurre en responsabilidad administrativa o no; puesto que la normativa específica otorga una mayor protección a los consumidores.

Por lo tanto, la primera instancia no debió exonerar de responsabilidad al proveedor si ya se había determinado que no cumplió con las obligaciones que establece la reglamentación en materia de servicios bancarios. No correspondía el análisis de la conducta de la consumidora incluso si a criterio de la autoridad administrativa esta podría haber sido imprudente o no.

Por otro lado, en segunda instancia, se determinó que, debido al incumplimiento del circuito de autenticación reforzada, la entidad bancaria incurre en infracción al deber de idoneidad. Sin embargo, la Comisión considera que no correspondía que la entidad bancaria active su sistema de monitoreo en tanto la operación fue la única realizada.

Sobre esto último, discrepo del criterio de la Comisión en tanto sí correspondía la activación del sistema de monitoreo para detectar operaciones que no sean acordes al patrón de la consumidora. Se alega que para conocer este concurren varios elementos que permiten concluir incluso cuando se trata de un consumo inusual, si es una primera y única operación, el Banco no tendría la obligación de generar una alerta.

Al respecto, es cierto que el patrón habitual de consumo se compone de múltiples factores como el tipo de comercio y el monto de las transacciones, entre otros.

Asimismo, las entidades bancarias cuentan con un historial de las operaciones de sus clientes a lo largo del tiempo y también cuentan con sistemas de monitoreo de estas operaciones. Por tanto, el criterio para determinar cuándo una operación es parte del patrón de consumo de un consumidor consiste en evaluar estos factores varios en función al historial de consumo.

Si bien el criterio que se utilizaba para dilucidar cuándo una operación no era habitual y si correspondía la activación de las medidas de seguridad era a partir de la segunda operación; en agosto de 2024, la Sala Especializada realizó un cambio de criterio.

Mediante el fundamento 34 de la Resolución N° 2293-2024/SPC-INDECOPI, se señala que: “para determinar si una operación es inusual o no al comportamiento habitual de consumo del cliente debe considerarse si, previamente, se realizaron, con cargo al producto estudiado, **operaciones por importes similares a los controvertidos** en sede administrativa.” (El resaltado es propio)

La Sala consideró como parámetro objetivo el importe individual de cada consumidor vinculado al producto o servicio materia de la controversia, es decir, si la consumidora no había realizado ninguna operación con un importe similar dentro de su historial de transacciones, se trataba de una operación inusual.

Con el cambio de criterio, la Sala en el fundamento 40 de la referida Resolución también recalca la obligación de las entidades financieras de implementar los medios tecnológicos que permitan corroborar que las operaciones sean acordes a los parámetros de ciberseguridad, pero también que se encuentren dentro de su patrón habitual de consumo.

Entonces, si bien es cierto que la Resolución de cambio de criterio fue posterior a la Resolución Final N° 1284-2024/CC1y puede ser objeto de crítica, considero que sí amerita que una operación que no encaje razonablemente en el patrón habitual de consumo de un consumidor no debería ser autorizada por la entidad bancaria, sino que debería desplegar la activación de las medidas de seguridad y monitoreo.

Así, la Comisión no sancionó a la entidad bancaria por haber autorizado una operación que no coincidía con el comportamiento usual de consumo de la consumidora, cuando sí correspondía que se pronuncie sobre tal extremo y no se limite a indicar de forma muy somera que por tratarse de una primera operación no corresponde la activación del sistema de monitoreo, incluso cuando esta primera operación excedía razonablemente cualquier consumo y/u operación realizada previamente por la consumidora.

Por último, la Comisión debió considerar que la entidad bancaria tampoco cumplió con las obligaciones establecidas en el artículo 22 del Reglamento de Tarjetas, en tanto no probó la incorporación de mecanismos para el seguimiento de operaciones vinculadas a fraude informático. Asimismo, no hizo mención del artículo 23 del Reglamento que directamente prevé la responsabilidad de la entidad bancaria ante las pérdidas que puedan sufrir los consumidores financieros.

Para concluir, el criterio de la Comisión en segunda instancia es el correcto, pero debió aplicar los artículos 22 y 23 del Reglamento de Tarjetas, así como haber sancionado a la entidad bancaria por no cumplir con activar su sistema de monitoreo en tanto la operación no encajaba con el patrón de consumo de la consumidora.

VI. CONCLUSIONES

- El Banco cometió una infracción al deber de idoneidad en tanto no pudo acreditar el cumplimiento del último paso del circuito de autenticación reforzada. Por tanto, el servicio brindado a la consumidora no cumplía con su finalidad ni con el sistema de garantías.
- Las principales obligaciones de la entidad bancaria en materia de operaciones no reconocidas por canal digital están comprendidas en el Código, pero específicamente en el artículo 17 y 22 del Reglamento de Tarjetas y en los artículos 18 y 19 del Reglamento de Ciberseguridad.

- Por tanto, las principales obligaciones consisten en implementar un sistema de monitoreo, así como en el fortalecimiento y cumplimiento del circuito de autenticación reforzada de las operaciones por canal digital.
- Un servicio o producto financiero ha sido brindado de manera idónea cuando se cumplen las garantías que establece el sistema de protección al consumidor: garantías legales, así como las ofrecidas expresamente por el proveedor y aquellas que son esperables conforme a los fines y usos previsibles.
- El criterio de la Comisión para sancionar al proveedor consistió en determinar que había incumplido con las obligaciones que establece la normativa sectorial. A diferencia del criterio de la OPS, la autoridad administrativa no analiza el comportamiento de la consumidora a efectos de intentar aplicar el artículo 104 del Código de Consumo.
- Adicionalmente, se ha considerado que el criterio de la Comisión fue el correcto; sin embargo, pudo haber aplicado los artículos 22 y 23 del Reglamento de Tarjetas, así como sancionar a la entidad bancaria por incumplimiento al deber de monitoreo.
- Finalmente, las garantías para un servicio idóneo consisten en las establecidas en la normativa de la SBS como en el Código de Consumo, así como en aquellas que fueron ofrecidas por los términos y condiciones, y por el contrato de consumo del servicio contratado; sin dejar de lado que el sistema financiero se sustenta también en garantías implícitas como la confianza en los mecanismos de seguridad bancarios para proteger el ahorro.

BIBLIOGRAFÍA

Constitución Política del Perú. (1993).

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. (2025). "Sistema financiero concentra el 90 % de sanciones por operaciones no reconocidas, revela Indecopi". Recuperado a partir de <https://www.gob.pe/institucion/indecopi/noticias/1150056-sistema-financiero-concentra-el-90-de-sanciones-por-operaciones-no-reconocidas-revela-indecopi>

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. (2018). Resolución N° 1332-2018/SPC-INDECOPI

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. (2024). Resolución Final N° 1284-2024/CC1

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. (2012). Resolución N° 2221-2012/SC2-Indecopi

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. (2023). Resolución Final N° 1881-2023/PS2

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. (2014). Resolución N° 2293-2024/SPC-INDECOPI

Ley N° 29571. Código de Protección y Defensa del Consumidor.

Resolución SBS. N° 6523-2013. Reglamento de Tarjetas de Crédito y Débito.

Resolución N° 504-2021. Que aprueba el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.

Superintendencia de Banca, Seguros y AFP. (2022). Boletín Semanal SBS Informa N° 24. “Autenticación reforzada: mayor seguridad para operaciones que puedan generar perjuicio al usuario”. Recuperado a partir de <https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1222>

Superintendencia de Banca, Seguros y AFP. (sf). *Información Estadística de Banca Múltiple*. Recuperado a partir de https://www.sbs.gob.pe/app/stats_net/stats/EstadisticaBoletinEstadistico.aspx?p=1#



ANEXOS





PERÚ

Presidencia
del Consejo de Ministros

INDECOPI

COMISIÓN DE PROTECCIÓN AL CONSUMIDOR N° 1
SEDE CENTRAL

EXPEDIENTE N° 2393-2023/PS2

RESOLUCIÓN FINAL N° 1284-2024/CC1

PROCEDENCIA : ÓRGANO RESOLUTIVO DE PROCEDIMIENTOS SUMARÍSIMOS DE PROTECCIÓN AL CONSUMIDOR N° 2 (OPS)

DENUNCIANTE : CECILIA XIMENA ARBRE BRAGA (SEÑORA ARBE)

DENUNCIADO : BANCO DE CRÉDITO DEL PERÚ S.A.¹ (BANCO)

MATERIAS : PROTECCIÓN AL CONSUMIDOR
DEBER DE IDONEIDAD
MEDIDA CORRECTIVA
GRADUACIÓN DE LA SANCIÓN
COSTAS Y COSTOS

ACTIVIDAD : SISTEMA FINANCIERO BANCARIO

SANCIÓN : **BANCO DE CRÉDITO DEL PERÚ S.A.: TRES CON SETENTA Y OCHO (3,78) UNIDADES IMPOSITIVAS TRIBUTARIAS (UIT)**

Lima, 5 de junio de 2024

ANTECEDENTES

1. Mediante escrito del 4 de setiembre de 2023, la señora Arbe denunció al Banco, por presuntas infracciones a la Ley N° 29571, Código de Protección y Defensa del Consumidor² (en adelante, Código), señalando lo siguiente:

- (i) El 12 de octubre de 2022 contrató con el Banco una Cuenta la Cuenta de Ahorros N° 191-*****-0-80, asociada a la Tarjeta de Débito N° 4557-***-***-7445.
- (ii) El 14 de julio de 2023, sufrió el robo de sus pertenencias, y fue víctima de fraude informático, a razón de lo cual se efectuó una operación no reconocida con cargo a su cuenta de ahorros, por lo que procedió a solicitar el bloqueo de sus tarjetas, así como una explicación sobre la operación no reconocida, y que se le brinde una solución ante lo ocurrido. El detalle de dicha operación fue el siguiente:

FECHA	CONCEPTO	IMPORTE
14-07-2023	Transferencia interbancaria	S/ 5 204.80

- (iii) Ante lo ocurrido, reclamó al Banco, quien el 17 de julio de 2023, le remitió una comunicación a través de la cual le indicó que era probable que a consecuencia del robo sufrido, una tercera persona haya accedido a sus cuentas, y haya efectuado la operación no reconocida materia de denuncia. Asimismo, le indicó que no era posible devolverle el importe de esta porque se habían realizado siguiendo los parámetros de seguridad.

¹ Con R.U.C. N° 20100047218

² Publicado el 2 de setiembre del 2010 en el Diario Oficial El Peruano, vigente a partir del 2 de octubre de 2010 y modificado por Decreto Legislativo N° 1308.

2. La señora Arbe solicitó, en calidad de medida correctiva, que el Banco devuelva el importe de la operación no reconocida materia de denuncia. Cabe precisar que requirió el reembolso de los costos y costas del procedimiento.
3. Por Resolución N° 1 del 11 de setiembre de 2023, el OPS admitió a trámite la denuncia presentada por la señora Arbe contra el Banco, formulando la siguiente imputación de cargos:

“(…)

PRIMERO: *Iniciar un procedimiento administrativo sancionador en mérito de la denuncia del 4 de setiembre de 2023, presentado por la señora Cecilia Ximena Arbe Braga contra Banco de Crédito del Perú por presunta infracción a lo establecido en los artículos 1° literal c) 18° y 19° del Código de Protección y Defensa del Consumidor, en tanto habría debitado indebidamente una (1) operación en su cuenta de ahorros N° 191-****0-08, la cual no reconoce, por los motivos expuestos en el numeral I.1 de la presente resolución:*

Fecha	Detalle	Importe S/
14/07/2023	TRANSF. BCO. SCOTIA B	5 240,80

4. El 18 de setiembre de 2023, la señora Arbe presentó los estados de cuenta de la cuenta de ahorros de su titularidad.
5. El 20 de setiembre de 2023, el Banco solicitó que se le concediera una prórroga del plazo otorgado para la presentación de sus descargos.
6. Por Resolución N° 2 del 17 de octubre de 2023, el OPS agregó al expediente los escritos presentados, los puso en conocimiento de las partes del procedimiento, y atendió la solicitud de prórroga del Banco.
7. El 19 de octubre de 2023, el Banco presentó su escrito de descargos, manifestando lo siguiente:
 - (i) La operación se dio válidamente con la información de seguridad de conocimiento exclusivo de la denunciante (número de Tarjeta Credimás N° 4557-****-****-8067, y su respectiva clave de internet, tal como se aprecia del reporte denominado “Operaciones BM”, mediante la glosa denominada “Login”.
 - (ii) La denunciante no ha alegado haber efectuado el bloqueo de su tarjeta antes de que se llevara a cabo la operación materia de denuncia, por lo que la operación se dio mientras esta se encontraba activa.
 - (iii) La denunciante reconoció no haber bloqueado su tarjeta, actuando de manera negligente, permitiendo así la realización de la operación materia de denuncia, lo cual configura una causal de ruptura del nexo causal que ocasiona que no se le pueda atribuir responsabilidad alguna por lo ocurrido.
8. Mediante Resolución N° 3 del 20 de octubre de 2023, el OPS agregó el escrito al expediente y lo puso en conocimiento de la otra parte.

9. Mediante Resolución Final N° 1881-2023/PS2 del 26 de octubre de 2023, el OPS emitió el siguiente pronunciamiento:

- (i) Declaró infundada la denuncia presentada contra el Banco, por la presunta infracción a lo establecido en el artículo 1° literal c), 18° y 19° del Código, por el presunto débito indebido de una operación en la cuenta de ahorros de la denunciante, sin que se verifique los incumplimientos adicionales alegados en la denuncia, y ras haberse verificado la ruptura del nexo causal por imprudencia de la consumidora:

Fecha	Detalle	Importe S/
14/07/2023	TRANSF. BCO. SCOTIA B	5 240,80

10. El 23 de noviembre de 2023, la señora Arbe interpuso un recurso de apelación contra la Resolución Final N° 1881-2023/PS2, manifestando lo siguiente:

- (i) El OPS señaló que el Banco no cumplió con el circuito de autenticación reforzada dispuesto por la normativa sectorial. No obstante, señaló que la operación se había dado por su negligencia la no reportar oportunamente el robo de sus pertenencias y bloquear su tarjeta.
- (ii) Resultaba errado exonerar de responsabilidad al Banco sobre la base de la ruptura del nexo causal, pues no había cumplido con el circuito de medidas de seguridad y ciberseguridad, establecidas en las normas sectoriales.
- (iii) El Banco no adoptó medias de seguridad idóneas, así como tampoco adoptó medidas para monitorear la operación materia de denuncia, en tanto esta no correspondía a su patrón habitual de consumo.

11. Mediante Resolución N° 4 del 30 de noviembre de 2023, el OPS concedió el recurso de apelación interpuesto por la señora Arbe contra la Resolución Final N° 1881-2023/PS2.

12. Por Memorandum N° 2016-2023-PS2/INDECOPI del 15 de diciembre de 2023, el OPS elevó el expediente a la Comisión de Protección al Consumidor N° 1 (en adelante, Comisión), en mérito al recurso de apelación interpuesto por la señora Arbe.

13. Mediante Resolución N° 1 del 19 de enero de 2024, la Secretaría Técnica de la Comisión (en adelante, Secretaría Técnica) puso en conocimiento del Banco el recurso de apelación interpuesto por la señora Arbe.

14. Mediante Resolución N° 2 del 10 de abril de 2024, la Secretaría Técnica efectuó el siguiente requerimiento de información:

“requerir a Banco del Crédito del Perú S.A. que, en el plazo improrrogable de tres (3) días hábiles, contado a partir del día siguiente de notificada la presente resolución, cumpla con lo siguiente:

- a. *En caso corresponda, presentar el medio probatorio pertinente que acredite el enrolamiento del denunciante en el canal digital, materia de cuestionamiento,*

aplicación del artículo 18° del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.

- b. Explicar de forma detallada cuáles son los dos (2) factores de autenticación reforzada de naturaleza distinta e independiente – contemplados en el literal j) del artículo 2 del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por Resolución SBS N° 504-2021 – utilizados por su representada en los supuestos de operación no reconocida realizada por canal digital, en aplicación del artículo 19° del citado reglamento; debiendo precisar, además, los motivos por los que considera que dichos factores son independientes entre sí y de distinta naturaleza.*
 - c. Detallar cuál es el código de autenticación y de uso único generado (mediante métodos criptográficos), a partir de los datos específicos de los supuestos de operación no reconocida realizada por canal digital.*
 - d. Presentar el medio probatorio pertinente que acredite que se notificó al usuario con los datos de los supuestos de operación no reconocida realizada por canal digital.*
 - e. Indicar si los supuestos de operación no reconocida realizada por canal digital se encuentran dentro del supuesto de exención de la norma; para lo cual, deberá explicar el límite y el cumplimiento de los requisitos exigibles para la aplicación de dicha exención, de conformidad con lo dispuesto en el artículo 20 del del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por Resolución SBS N° 504-2021.*
 - f. En caso corresponda, explicar de forma detallada el cumplimiento de lo dispuesto en el literal d) del numeral 17.1 del artículo 17° y en el numeral 17.4 del artículo 17° del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, relacionado con la implementación de procesos de autenticación para controlar el acceso a los servicios que se proveen a los usuarios por canales digitales sobre línea base de controles de seguridad de la información requerida y la existencia de herramientas y procedimientos para implementar el monitoreo de transacciones que permita tomar medidas de reducción de la posibilidad de operaciones fraudulentas; lo cual deberá acompañarse de los medios probatorios con los que se acredita el referido cumplimiento, así como una explicación detallada de los mecanismos, reportes y las glosas que permiten verificar lo indicado.*
 - g. En caso se alegue que, en el presente caso, se efectuó registro de un beneficiario de confianza, modificación en los productos de seguro ahorro/inversión contratados, la contratación de un producto o servicio, modificación de límites y condiciones u otro supuesto recogido en el artículo 19 del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por Resolución SBS N° 504-2021, brindar la información pertinente a los puntos a, b, c, d, e, f. (...)"*
15. El 17 de abril de 2024, el Banco absolvió el requerimiento de información que le fuera efectuado, en los siguientes términos:
- (i) Respecto del punto (a), obraba en el expediente copia del documento denominado "Reporte de Afiliación del dispositivo móvil ID N° 44457616. Sin perjuicio de ello, debía considerarse que la denunciante no había desconocido haberse afiliado a la clave de internet ni a la clave token, ni a la banca móvil.

- (ii) Respecto del punto (c), el código de autenticación es la clave token generada por una semilla criptográfica a base de un algoritmo que impide ser adivinado por terceros o por el mismo cliente.
 - (iii) Respecto del punto (d), se había adjuntado el reporte denominado "Constancia". Sin perjuicio de ello, debía precisar que cualquier cuestionamiento relacionado a la falta de notificación no desvirtúa la validez de la operación.
 - (iv) Respecto de los puntos (b), (e), (f) y (g), debía indicarse que el Indecopi carecía de competencia para verificar el cumplimiento de las medidas de Ciberseguridad. La autoridad competente para verificar ello era la Superintendencia de Banca, Seguros & AFP.
16. Por Resolución N° 3 del 30 de mayo de 2024, se agregó el escrito al expediente y fue puesto en conocimiento de la denunciante.

ANALISIS

Cuestión previa: sobre la competencia del Indecopi

17. El artículo 105° del Código establece que el Indecopi es la autoridad con competencia primaria y de alcance nacional para conocer las presuntas infracciones a las disposiciones contenidas en el presente Código, así como para imponer las sanciones y medidas correctivas establecidas en el presente capítulo, conforme a la Ley de Organización y Funciones del Indecopi, aprobada por Decreto Legislativo N° 1033.
18. Dicha normativa también dispone también que la competencia del Indecopi solo puede ser negada cuando ella haya sido asignada o se asigne a favor de otro organismo por norma expresa con rango de ley³.
19. De otro lado, el Código Procesal Civil, de aplicación supletoria a los procedimientos administrativos, establece en el numeral 4 del artículo 427, que el juez declarará improcedente la demanda cuando carezca de competencia⁴.
20. En el presente caso, mediante escrito del 17 de abril de 2024, el Banco señaló que el Indecopi carece de competencia para indagar sobre aspectos técnicos del Reglamento de Ciberseguridad o para determinar el cumplimiento de las obligaciones contenidas en dicha norma, siendo la entidad competente la SBS.

³ **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de setiembre de 2010 y modificado por Decreto Legislativo N° 1308.**

Artículo 105.- Autoridad competente

El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi) es la autoridad con competencia primaria y de alcance nacional para conocer las presuntas infracciones a las disposiciones contenidas en el presente capítulo, conforme al Decreto legislativo núm. 1033, Ley de Organización y Funciones del Indecopi. Dicha competencia solo puede ser negada cuando ella haya sido asignada o se asigne a favor de otro organismo por norma expresa con rango de ley. (...)

⁴ **TEXTO ÚNICO ORDENADO DEL CÓDIGO PROCESAL CIVIL, aprobado por Resolución Ministerial 010-93-JUS y publicado el 22 de abril de 1993**

Artículo 427.- El juez declarará improcedente la demanda cuando:

(...)

4. Carezca de competencia.

21. Sobre el particular, cabe señalar que, en materia de productos y servicios financieros, el Código dispone una serie de obligaciones –contenidas entre los artículos 82° y 90° del mencionado cuerpo legal– que deben ser cumplidas por las empresas supervisadas por la SBS teniendo en cuenta las normas que dicha entidad emita en el marco de sus facultades regulatorias.
22. Asimismo, el artículo 81° del Código⁵ dispone que la regulación y supervisión del sistema financiero, así como de los productos y servicios, se rigen, en virtud del principio de especialidad normativa, por la Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, cuya implementación se encuentra regulada a través de diversos reglamentos y circulares emitidos por la SBS, como el Reglamento de Sanciones Aplicadas a las Personas Naturales y Jurídicas Supervisadas (en adelante, el Reglamento de Sanciones), aprobado por Resolución SBS 816-2005.
23. El artículo 19° del Reglamento de Sanciones⁶ señala que será la SBS la entidad competente para conocer los incumplimientos de las disposiciones que rigen a las empresas supervisadas en su relación directa con el cliente cuando constituyan un patrón de conducta, conforme a las atribuciones que le han sido conferidas por su ley orgánica; asimismo, establece que los casos individuales que contengan materia amparada por las normas de protección al consumidor serán derivados al Indecopi.
24. De igual forma, la Sala Especializada en Protección al Consumidor (en adelante, la Sala), mediante la Resolución N° 1332-2018/SPC-INDECOPI, al analizar su competencia para conocer de infracciones que pudieran también ser conocidas por la Superintendencia de Banca, Seguros y AFP, señaló lo siguiente:

“42. Por otro lado, esta Sala hace notar que, de los actuados, no se advierte vulneración al principio non bis in ídem, en la medida que la SBS y el Indecopi tutelan bienes jurídicos distintos, siendo que la primera entidad tutela fundamentalmente el

⁵ **LEY 29571 MODIFICADO POR EL DECRETO LEGISLATIVO 1308 DEL 30 DE DICIEMBRE DE 2016. CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR.**

Artículo 81°. –

La materia de protección al consumidor de los servicios financieros prestados por las empresas supervisadas por la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones se rige por las disposiciones del presente Código, así como por las normas especiales establecidas en la Ley núm. 28587, Ley Complementaria a la Ley de Protección al Consumidor en Materia de Servicios Financieros, y las normas reglamentarias emitidas para garantizar su cumplimiento. La regulación y supervisión del sistema financiero, así como los productos y servicios se rige en virtud del principio de especialidad normativa por la Ley núm. 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.

⁶ **RESOLUCIÓN SBS 816-2005. REGLAMENTO DE SANCIONES APLICADAS A LAS PERSONAS NATURALES Y JURÍDICAS SUPERVISADAS. TÍTULO V. PROCEDIMIENTO SANCIONADOR.**

Artículo 19.-

Inicio y partes del procedimiento. El procedimiento sancionador se inicia siempre de oficio, sobre la base de los hechos detectados por la propia Superintendencia u otras entidades o por las denuncias presentadas por terceros al amparo del artículo 105 de la Ley del Procedimiento Administrativo General. En el procedimiento sancionador sólo participan la Superintendencia y la o las personas a las que se les imputa la comisión de una infracción administrativa. La persona que denuncia un hecho que considera contrario al ordenamiento legal conforme a lo indicado en el párrafo anterior, no forma parte del procedimiento sancionador, teniendo derecho únicamente a que se le notifique el resultado del mismo. En el caso de denuncias sobre el incumplimiento de las disposiciones que rigen a las empresas supervisadas en su relación directa con los clientes, la Superintendencia ejercerá su potestad sancionadora cuando éstas constituyan un patrón de conducta, conforme a las atribuciones que le han sido conferidas por su ley orgánica. Los casos individuales que contengan materia amparada por las normas de protección al consumidor, serán derivados al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).

funcionamiento y operatividad del sistema financiero, y el Indecopi los derechos de los consumidores con relación a los productos o servicios que adquieren, utilizan o disfrutan.”

25. Por tanto, se aprecia que los bienes jurídicos tutelados por ambas entidades difieren, en tanto persiguen finalidades distintas, pues la SBS, no se encarga de velar por la afectación de los intereses particulares de los consumidores, lo cual sí es competencia del Indecopi.
26. En tal sentido, el Indecopi resulta ser la entidad competente para conocer la conducta cuestionada por la señora Arbe, referida a la presunta no adopción de medidas de seguridad para la realización de la operación no reconocida con cargo a su cuenta de ahorros; en tanto, el hecho discutido se encuentra vinculado con una afectación a los intereses particulares del consumidor.
27. Si bien el proveedor denunciado alega que el Indecopi carece de competencia para indagar sobre aspectos técnicos del Reglamento de Ciberseguridad o para determinar el cumplimiento de las obligaciones contenidas en dicha norma porque la entidad competente es la SBS, lo cierto es que el Indecopi —durante la etapa de instrucción o a través de sus órganos resolutivos—, tiene la facultad de requerir a las entidades supervisoras o reguladoras opiniones técnicas con respecto a la normativa que estas regulan con la finalidad de emitir un pronunciamiento acorde a derecho.
28. Además, debe tenerse en consideración que el Indecopi se encuentra en la obligación de resolver las denuncias que se presenten ante esta institución en concordancia con lo que dispone el ordenamiento jurídico, en consecuencia, no podría dejar de aplicar la normativa sectorial emitida por la SBS, en concreto, el Reglamento de Ciberseguridad, en la medida que estas establecen cuales son las medidas de seguridad que deben adoptar las entidades del sector bancario bancario-financiero para las operaciones realizadas mediante un canal digital.
29. En esa medida, cuando un consumidor denuncie ante esta institución que se realizaron operaciones no reconocidas en su perjuicio, el Indecopi está obligado a constatar lo que establece el Reglamento de Ciberseguridad para determinar si el proveedor denunciado cumplió con las exigencias que le ha impuesto tal norma, lo contrario sería desconocer lo que la autoridad en la materia ha reglamentado y regulado; por lo que, contrariamente a lo alegado por el Banco en su escrito del 17 de abril de 2024, con el requerimiento efectuado a través de la Resolución N° 2 no se asume que el Banco no ha cumplido con las medidas de seguridad, sino, en realidad, se busca tener la información correspondiente para que, posteriormente, se emita un pronunciamiento debidamente motivado, en tanto esta es la normativa sectorial aplicable al presente caso.
30. Tal es así que, en diversos procedimientos, incluso de los que ha formado parte la entidad bancaria, la Secretaría Técnica ha recurrido a lo dispuesto por la SBS a efectos de verificar si se ha cumplido con lo señalado en la normativa de la materia; esto es relevante porque permitirá determinar si el denunciado ha regulado su conducta con las obligaciones que establece la norma.
31. No podría alegarse, por ejemplo, que la autoridad solo podría aplicar una norma en particular y otra no, cuando tal normativa resulta aplicable a un solo hecho; en efecto, si

el ordenamiento jurídico vigente establece diversos supuestos normativos a los que el administrado se encuentra obligado a cumplir, es deber de la autoridad verificar —en el marco de un procedimiento sancionador, como en el presente caso— que tal ordenamiento se cumpla. Una evaluación completa del ordenamiento jurídico vigente permitirá a la autoridad emitir un pronunciamiento motivado y fundamentado en derecho.

32. Por los argumentos expuestos, sí tiene competencia para verificar los hechos denunciados en el presente procedimiento y verificar la normativa que resulta relevante para la materia, por lo que se desestima lo alegado por la entidad bancaria.

Sobre la presunta infracción al deber de idoneidad

33. El artículo 18° del Código establece que la idoneidad es la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe⁷.
34. Por su parte, el artículo 19° del Código establece que los proveedores son responsables por la calidad e idoneidad de los productos y servicios que ofrecen en el mercado⁸. En aplicación de esta norma, los proveedores tienen el deber de entregar los productos y prestar los servicios al consumidor en las condiciones ofertadas o previsibles, atendiendo a la naturaleza de estos, la regulación que sobre el particular se haya establecido y, en general, a la información brindada por el proveedor o puesta a disposición.
35. Asimismo, el literal c) del artículo 1° del Código⁹ señala que es un derecho de los consumidores, la protección de sus intereses económicos y en particular contra las cláusulas abusivas, métodos comerciales coercitivos, cualquier otra práctica análoga e información interesadamente equívoca sobre los productos o servicios.

— De las medidas de seguridad aplicables a las operaciones

⁷ **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de setiembre de 2010 y modificado por el Decreto Legislativo N° 1308, publicado en el Diario Oficial El Peruano el 30 de diciembre de 2016.**

Artículo 18.- Idoneidad

Se entiende por idoneidad la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe, en función a lo que se le hubiera ofrecido, la publicidad e información transmitida, las condiciones y circunstancias de la transacción, las características y naturaleza del producto o servicio, el precio, entre otros factores, atendiendo a las circunstancias del caso.

(...)

⁸ **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de setiembre de 2010 y modificado por el Decreto Legislativo N° 1308, publicado en el Diario Oficial El Peruano el 30 de diciembre de 2016.**

Artículo 19.- Obligación de los proveedores

El proveedor responde por la idoneidad y calidad de los productos y servicios ofrecidos; por la autenticidad de las marcas y leyendas que exhiben sus productos o del signo que respalda al prestador del servicio, por la falta de conformidad entre la publicidad comercial de los productos y servicios y estos, así como por el contenido y la vida útil del producto indicado en el envase, en lo que corresponda.

⁹ **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de setiembre de 2010 y modificada por el DECRETO LEGISLATIVO 1308, publicado el 30 de diciembre de 2016**

Artículo 1.- Derechos de los consumidores

1.1 En los términos establecidos por el presente Código, los consumidores tienen los siguientes derechos:

(...)

c. Derecho a la protección de sus intereses económicos y en particular contra las cláusulas abusivas, métodos comerciales coercitivos, cualquier otra práctica análoga e información interesadamente equívoca sobre los productos o servicios.

36. Sobre el particular, la relación jurídica que se genera entre una entidad financiera y un consumidor como consecuencia de la entrega de una tarjeta de crédito o débito crea deberes y derechos para ambas partes. Entre las obligaciones del consumidor, están la de custodiar adecuadamente su tarjeta, mantener la confidencialidad de su clave secreta, comunicar a la entidad financiera sobre el robo, hurto o extravío de la tarjeta, entre otros.
37. En cuanto a las obligaciones de las entidades financieras, una condición implícita en los servicios financieros ofertados en el mercado, integrada a su idoneidad, es la garantía otorgada por los proveedores de que adoptarán las medidas de seguridad que fueran necesarias para garantizar que el patrimonio de los consumidores se encuentre debidamente resguardado. En ese sentido, debe entenderse que parte del servicio prestado por el Banco, implica la confianza que el consumidor deposita en los sistemas de seguridad con los que cuenta la institución financiera para la realización y aprobación de cualquier transacción comercial realizada a través de tarjetas de crédito o débito que afecte su patrimonio.
38. Por ello, en el marco de la relación comercial existente entre los consumidores y las entidades del sistema financiero, se exige a estas la implementación de mecanismos de seguridad destinados a proteger las transacciones que realizan sus clientes, evitando el uso indebido o fraudulento de las tarjetas de crédito o débito.
39. En esa línea, el artículo 9° del Reglamento, establece que las entidades bancarias únicamente podrán cargar en las cuentas de las tarjetas de crédito de los tarjetahabientes el importe de los bienes y servicios que adquieran utilizándolas, de acuerdo a las órdenes de pago que estos autoricen, o por autorizaciones realizadas a través de medios electrónicos y/o firmas electrónicas, así como por autorizaciones expresas y previamente concedidas por el titular de la tarjeta de crédito¹⁰.
40. Dicha disposición también aplica a las tarjetas de débito, según lo indicado en el artículo 14° del Reglamento, el cual establece que las entidades bancarias únicamente podrán cargar en las cuentas de las tarjetas de débito de los tarjetahabientes el importe de los bienes y servicios que adquieran utilizándolas, de acuerdo con las órdenes de pago que autoricen¹¹. Asimismo, la norma contempla la posibilidad que, de ser el caso, dichas

¹⁰ **RESOLUCIÓN SBS N° 6523-2013. REGLAMENTO DE TARJETAS DE CRÉDITO Y DÉBITO, publicada el 2 de noviembre de 2013 y vigente desde el 1 de abril de 2014**

Artículo 9°.- Cargos

Las empresas cargarán el importe de los bienes, servicios y obligaciones que el usuario de la tarjeta de crédito adquiera o pague utilizándola, de acuerdo con las órdenes de pago que este autorice; el monto empleado como consecuencia del uso de alguno de los servicios descritos en el artículo 7 del Reglamento, en caso corresponda; así como las demás obligaciones señaladas en el contrato de tarjeta de crédito, conforme a la legislación vigente sobre la materia.

Las órdenes de pago y firmas podrán ser sustituidas por autorizaciones a través de medios electrónicos y/o firmas electrónicas sujetas a verificación por las empresas, entidades que esta designe o por las entidades acreditadas para tal efecto, conforme al marco normativo aplicable, así como por autorizaciones expresas y previamente concedidas por el titular de la tarjeta de crédito.

¹¹ **RESOLUCIÓN SBS N° 6523-2013, REGLAMENTO DE TARJETAS DE CRÉDITO Y DÉBITO, publicada el 2 de noviembre de 2013 y vigente desde el 1 de abril de 2014**

Artículo 14°.- Cargos

Las empresas cargarán el importe de los bienes, servicios y obligaciones que el usuario de la tarjeta de débito adquiera o pague utilizándola, de acuerdo con las órdenes de pago que este autorice; el monto empleado como consecuencia del

órdenes sean reemplazadas por autorizaciones o firmas electrónicas.

41. Del análisis de dicha norma, se desprende que lo que busca garantizar es que, en cualquiera de los escenarios en que se realice la operación de consumo, esta se haya efectuado en observancia de las medidas de seguridad correspondientes, por lo cual se exige a las entidades financieras contar con el sustento que acredite de manera indubitable la autorización realizada por el cliente, sea a través de la suscripción de una orden de pago, el ingreso de un código o la firma de manera electrónica y/o virtual (clave secreta, clave dinámica, CVV, etc.).
42. En la dinámica común del mercado existen diversos tipos de operaciones que pueden realizarse con tarjetas de crédito o débito, siendo que para algunas se requiere la presencia física del medio de pago (plástico) y en otros casos no, por lo que pueden realizarse operaciones “con tarjeta presente” y “con tarjeta no presente”. Para garantizar que este tipo de operaciones se realicen válidamente, con la autorización del tarjetahabiente, las entidades financieras deben adoptar medidas de seguridad específicas.
43. En esa línea, para el caso de operaciones “con tarjeta presente”, es necesario que, para poder realizar una transacción, se cuente con la presencia física de la tarjeta, la cual es pasada por un terminal de venta (o POS, por sus siglas en inglés, Point of Sale), requiriéndose, según el caso, la firma electrónica (clave secreta) o la suscripción de la orden de pago, para que pueda entenderse como autorizada. Así también, existen otras operaciones que no requieren que la tarjeta sea leída por un terminal POS, pero sí el ingreso de la firma electrónica, como por ejemplo las disposiciones de efectivo a través de cajero automático¹².
44. Con relación a las operaciones “con tarjeta no presente”¹³, no se requiere la presencia de la tarjeta de crédito física, solicitándose que la autorización se realice a través de medios electrónicos, como por ejemplo vía internet en el que se requiere el ingreso de datos impresos en el medio de pago, tales como fecha de vencimiento y el código CVV, con lo que se verifica la autorización del cliente.

uso de alguno de los servicios descritos en el artículo 13° del Reglamento, en caso corresponda; así como las demás obligaciones señaladas en el contrato de tarjeta de crédito, conforme a la legislación vigente sobre la materia.

Las órdenes de pago y firmas podrán ser sustituidas por autorizaciones a través de medios electrónicos y/o firmas electrónicas sujetas a verificación por las empresas, entidades que esta designe o por las entidades acreditadas para tal efecto, conforme al marco normativo aplicable, así como por autorizaciones expresas y previamente concedidas por el titular de la tarjeta de débito.

¹² Ver de manera ilustrativa, la página web de Visa: <<http://www.visaeurope.es/visa-para-comercios/seguridad/transacciones-visa/tarjeta-presente/>> en la cual se refiere a las operaciones a través de tarjeta presente conforme a lo siguiente: “(...) son las transacciones que se realizan cara a cara, cuando la tarjeta Visa y su titular están presentes físicamente en la caja o terminal de un establecimiento o comercio”.

¹³ Ver de manera ilustrativa, la página web de Visa: <<http://www.visaeurope.es/visa-para-comercios/seguridad/transacciones-visa/tarjeta-no-presente/>> en la cual se refiere a las operaciones a través de tarjeta no presente de la siguiente manera: “Las compras con tarjeta no presente tienen lugar a distancia – a través de Internet, por teléfono o por correo postal. Las tarjetas (...) son especialmente adecuadas para este tipo de transacciones, al hacer más eficiente el proceso de compra, sustituyendo otros más engorrosos como el pago contra reembolso o mediante factura. (...) Código de Seguridad de la tarjeta.

El código de seguridad de tres dígitos que aparece en el reverso de cada tarjeta Visa. Su denominación técnica en inglés es Card Verification Code 2 (CVV2) o Código de Verificación de la Tarjeta 2. Visa Europe estima que verificar el código de seguridad de las tarjetas puede ayudar a recortar la tasa de fraude hasta en un 70%”.

45. Esto quiere decir, que, ante el cuestionamiento de un consumidor, la entidad financiera debe estar en la posibilidad de acreditar de manera fehaciente que la operación cargada ha sido autorizada por el cliente¹⁴.

Tratamiento de operaciones realizadas a través de canales digitales

46. Los artículos 7 y 13 del Reglamento de Tarjetas, establecen que las entidades bancarias ofrecen servicios relacionados con operaciones de tarjetas de crédito y tarjetas de débito que adquieran los usuarios y, adicionalmente, los tarjetahabientes podrán realizar operaciones a través de internet, páginas web y/o aplicaciones de dispositivos móviles, entre otros, distintos a los provistos por la empresa¹⁵.

¹⁴ En esa misma línea, mediante Oficio N° 26791-2017-SBS del 3 de agosto de 2017 dirigida a la Secretaría Técnica de la Comisión, la Superintendencia de Banca, Seguros y AFP precisó los alcances del artículo 9° del Reglamento, señalando lo siguiente:

“Visto así, (...) para su defensa la entidad financiera debe presentar el voucher suscrito por el cliente para acreditar el cargo de la operación, o en caso de micropago, demostrar la responsabilidad del usuario.”

Sin perjuicio de lo anterior, el artículo 9° del Reglamento permite a la empresa sustituir el voucher suscrito por el cliente por autorizaciones a través de medios electrónicos y/o firmas electrónicas (...). La finalidad de dicha precisión (...) es permitir la verificación adecuada de la operación y de su autorización por parte del cliente en la realización de transacciones por canales no presenciales, por ejemplo, internet, donde no resulta posible solicitar, al momento de la operación, la impresión de una orden de pago y su suscripción por parte del cliente.”

(Subrayado nuestro)

¹⁵ **RESOLUCIÓN SBS N° 6523-2013. REGLAMENTO DE TARJETAS DE CRÉDITO Y DÉBITO, publicada el 2 de noviembre de 2013, vigente desde el 1 de abril de 2014 y modificado por Resolución SBS N° 5570-2019 publicada el 27 de noviembre de 2019.**

Artículo 7. – Servicios adicionales asociados a las tarjetas de crédito

Las empresas pueden ofrecer los siguientes servicios adicionales:

1. Disposición de efectivo otorgando al titular la posibilidad de elegir, para cada operación, si la disposición será financiada en cuotas, y de ser el caso, decidir el número de cuotas.
2. Operaciones realizadas a través de internet, desde páginas web y/o aplicaciones de dispositivos móviles, entre otros, distintos a los provistos por la empresa
3. Operaciones efectuadas en el exterior de forma presencial
4. Sobregiro o exceso de la línea de crédito.

La posibilidad de incorporar estos servicios se debe informar de manera previa a la celebración del contrato, y el titular debe estar en posibilidad de habilitarlos, al momento de la contratación o de forma posterior, y deshabilitarlos en el momento que así lo requiera, aspecto que también debe ser informado. Los mecanismos para la deshabilitación de los servicios no podrán ser más complejos que aquellos empleados para su habilitación. Las empresas no pueden incorporar los servicios adicionales sin el consentimiento previo del titular.

Las empresas que ofrezcan los servicios descritos deben de informar a los usuarios las condiciones aplicables y riesgos asociados a su utilización, incluidas las medidas de seguridad que deben observar los usuarios, para el uso de dichos servicios en cualquiera de los medios o canales, como cajeros automáticos, páginas web, dispositivos móviles, entre otros, según corresponda.

(...)

Artículo 13.- Servicios adicionales asociados a tarjetas de débito

Las empresas pueden ofrecer los siguientes servicios adicionales:

1. Operaciones realizadas a través de internet, desde páginas web y/o aplicaciones de dispositivos móviles, entre otros, distintos a los provistos por la empresa.
2. Operaciones efectuadas en el exterior de forma presencial.

La posibilidad de incorporar estos servicios se debe informar de manera previa a la celebración del contrato, y el titular debe de estar en posibilidad de habilitarlos, al momento de la contratación o de forma posterior, y de deshabilitarlos en el momento que así lo requiera, aspecto que también debe ser informado. Los mecanismos para la deshabilitación de los servicios no podrán ser más complejos que aquellos empleados para su habilitación. Las empresas no pueden incorporar los servicios adicionales sin el consentimiento previo del titular.

47. El artículo 15 del Reglamento de Tarjetas establece las medidas de seguridad incorporadas en las tarjetas, señalando que el procesamiento de transacciones en línea que usa el chip de las tarjetas u otros mecanismos de seguridad debe incluir: (i) la solicitud de autorización realizada; (ii) la respuesta a la solicitud generada desde el sistema autorizador de la empresa; y, (iii) la indicación de haber aprobado o declinado la transacción generada, salvo en caso de excepción prevista contractualmente.
48. En esa misma línea, se dispuso que cuando las operaciones se realicen con el uso del chip u otro mecanismo sin contacto, se requerirá que la autenticación de la tarjeta debe utilizar criptografía dinámica, a fin de verificar que no hubo alteración de la transacción entre la tarjeta y el terminal. Además, en caso se utilice un soporte distinto a la tarjeta física, aparte de asegurar los mecanismos de autenticación, se debe evitar exponer el número de la tarjeta¹⁶.
49. De la lectura de la norma citada, se concluye que el Reglamento de Tarjetas busca garantizar que las operaciones efectuadas a través de cualquier medio —lo que incluye el canal digital— se realicen en observancia de las medidas de seguridad correspondientes al canal por el que estas se efectúan; por lo que, se exige a las entidades que cuenten con el sustento que acredite de manera indubitable la autorización otorgada por el usuario.

Sobre el Reglamento de Ciberseguridad aplicable para operaciones realizadas por canal digital

Las empresas que ofrezcan los servicios descritos deben de informar a los usuarios las condiciones aplicables y riesgos asociados a su utilización, incluidas las medidas de seguridad que deben observar los usuarios para el uso de dichos servicios en cualquiera de los medios o canales, como cajeros automáticos, páginas web, dispositivos móviles, entre otros, según corresponda.

¹⁶ **RESOLUCIÓN SBS N° 6523-2013. REGLAMENTO DE TARJETAS DE CRÉDITO Y DÉBITO, publicada el 2 de noviembre de 2013, vigente desde el 1 de abril de 2014 y modificado por Resolución SBS N° 5570-2019 publicada el 27 de noviembre de 2019.**

Artículo 15. – Medidas de seguridad incorporadas en las tarjetas

Las tarjetas deberán contar con un circuito integrado o chip que permita almacenar y procesar la información del usuario y sus operaciones, cumpliendo estándares internacionales de interoperabilidad para el uso y verificación de las tarjetas, así como para la autenticación de pagos; para lo cual deberá cumplirse como mínimo con los requisitos de seguridad establecidos en el estándar EMV, emitido por EMVCo. Al respecto, las empresas deberán aplicar, entre otras, las siguientes medidas:

1. Reglas de seguridad definidas en el chip de las tarjetas, que deben ser utilizadas para verificar la autenticidad de la tarjeta, validar la identidad del usuario mediante el uso de una clave o firma u otros mecanismos de autenticación.
2. Aplicar procedimientos criptográficos sobre los datos críticos y claves almacenadas en el chip de las tarjetas, así como sobre aquellos existentes en los mensajes intercambiados entre las tarjetas, los terminales de punto de venta, los cajeros automáticos y las empresas emisoras.
3. En caso las empresas emisoras permitan la autorización de operaciones fuera de línea, deben aplicar un método de autenticación de datos que brinde adecuadas condiciones de seguridad, sin afectar la calidad y el rendimiento del servicio provisto al usuario. Dichas operaciones se realizarán conforme a los límites y condiciones pactadas con el cliente, que incluirán por ejemplo límites al número de operaciones consecutivas procesadas fuera de línea.
4. Disponer de mecanismos para aplicar instrucciones sobre el chip de las tarjetas en respuesta a una transacción en línea, a fin de modificar los límites establecidos según perfiles de riesgo, así como bloquear o deshabilitar aquellas tarjetas que hayan sido extraviadas o sustraídas.

El procesamiento de transacciones en línea haciendo uso del chip de las tarjetas u otros mecanismos debe incluir como mínimo la solicitud de autorización realizada, la respuesta a la solicitud, la cual debe ser generada desde el sistema autorizador de la empresa, así como la indicación de haber aprobado o declinado la transacción generada; ello salvo en caso de excepción previsto contractualmente, donde corresponda la aprobación a la marca. Cuando la operación sea realizada haciendo uso del chip u otro mecanismo sin contacto, la autenticación de la tarjeta debe utilizar criptografía dinámica, de manera que pueda verificarse que no hubo alteración de la transacción entre la tarjeta y el terminal. Cuando se utilice otro soporte distinto a la tarjeta física, además de asegurar mecanismos de autenticación, debe evitar exponer el número de la tarjeta.

50. La creciente interconectividad y mayor adopción de canales digitales para la provisión de los servicios, así como la virtualización de determinados productos del sistema financiero, de seguros y privado de pensiones, generó la necesidad en las empresas de fortalecer sus capacidades de ciberseguridad y procesos de autenticación.
51. Así, la SBS publicó el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por Resolución SBS N° 504-2021 (en adelante, Reglamento de Ciberseguridad), cuyas disposiciones legales contienen un marco de referencia para el sistema de gestión de seguridad de la información, el cual tiene por finalidad fortalecer las capacidades de ciberseguridad y procesos de autenticación por parte de las empresas supervisadas por la SBS para la realización de operaciones en un entorno seguro y confiable.
52. Al respecto, la norma tiene dos (2) características: a) un carácter subjetivo, referido a las partes obligadas a cumplir con las disposiciones de la referida normativa pertenecientes al régimen general y simplificado; y, b) un carácter objetivo, que establece la vigencia y el tipo de operaciones objeto de regulación. Así, se observa que el Reglamento de Ciberseguridad entró en vigor el 1 de julio de 2021¹⁷; sin embargo, algunas disposiciones entraron en vigencia de manera posterior.
53. En efecto, el Reglamento de Ciberseguridad precisó que las disposiciones señaladas en el Subcapítulo III del Capítulo II referido a los procesos de enrolamiento y autenticación y la Tercera Disposición Complementaria Final¹⁸ referido a reportes de incidentes de ciberseguridad significativos, tenían un plazo de adecuación hasta el 2 de

¹⁷ **RESOLUCIÓN SBS N° 504-2021, REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD, publicada el 19 de febrero de 2021**

Artículo Décimo. – Vigencia

La presente Resolución entra en vigencia el 1 de julio de 2021, fecha en la que se deroga la Circular G 140-2009, con excepción de lo siguiente:

- a. Los párrafos 25.1 y 25.2 del artículo 25 del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por el Artículo Primero, que entran en vigencia al día siguiente de publicada la presente Resolución, fecha en la cual se deroga el artículo 7A de la Circular G 140-2009.
- b. El Artículo Segundo de la presente Resolución entra en vigencia a partir de la auditoría correspondiente al ejercicio 2022.
- c. Los Artículos Séptimo, Octavo y Noveno de la presente Resolución, entran en vigencia al día siguiente de la publicación de la presente Resolución, con excepción de lo indicado en el inciso d. del presente Artículo.
- d. El requerimiento asociado a la inclusión conjunta de la información sobre la denominación social de la empresa emisora y el nombre comercial que la empresa asigne al producto de tarjeta de crédito y/o débito, señalado en el Artículo Séptimo de la presente Resolución, así como el requerimiento asociado a la inclusión de la dicha información en los dispositivos de soporte al dinero electrónico, señalado en el artículo Octavo de la presente Resolución; entran en vigencia el 1 de enero de 2022.

¹⁸ **RESOLUCIÓN SBS N° 504-2021, REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD, PUBLICADA EL 19 DE FEBRERO DE 2021**

**CAPÍTULO II SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD (SGSI-C)
SUBCAPÍTULO III AUTENTICACIÓN**

(...)

DISPOSICIONES COMPLEMENTARIAS FINALES

TERCERA. - En caso de eventos que afecten la continuidad operativa y que tengan como causa probable un incidente de seguridad de la información, es aplicable lo señalado en el artículo 15 del Reglamento para la Gestión de la Continuidad del Negocio, aprobado por la Resolución SBS N° 877-2020, sobre reporte de eventos de interrupción significativa

julio de 2022¹⁹; siendo aplicable a partir de dicha fecha para las empresas supervisadas por la SBS.

54. Por consiguiente, se puede concluir que el Reglamento de Ciberseguridad resulta de aplicación obligatoria a las empresas que integran el Régimen General y el Régimen Simplificado a partir del 2 de julio de 2022, respecto a los procesos de enrolamiento y autenticación de los usuarios en los servicios que brinden las empresas.
55. En esa línea de ideas, respecto del ámbito de aplicación, resulta necesario señalar lo expuesto en el Reglamento de Ciberseguridad. El artículo 17° de dicha disposición legal establece que las empresas que brindan servicios a sus usuarios por canales digitales deben considerar determinados factores de autenticación a fin de prevenir amenazas a la seguridad de la información²⁰.
56. Para tal efecto, el artículo 18° del Reglamento de Ciberseguridad señala que, el enrolamiento del usuario para el uso de canales digitales requiere por lo menos: a) verificar la identidad del usuario y tomar las medidas necesarias para reducir la posibilidad de suplantación de identidad, lo que incluye el uso de dos factores independientes de categorías diferentes²¹; y, b) generar las credenciales y asignarlas al usuario.
57. En esa misma línea, el artículo 19° de la referida norma, establece que se requiere de **autenticación reforzada** para aquellas acciones que puedan generar operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente como las operaciones a través de un canal digital que impliquen pagos o transferencia de fondos a terceros, registro de un beneficiario de confianza, modificación en los productos de seguro ahorro/inversión contratados, la contratación de un producto o servicio, modificación de límites y condiciones²².

¹⁹ Ver la información detallada en el Boletín Semanal SBS Informa N° 7 de marzo de 2021, respecto a la Seguridad de la Información y Ciberseguridad, en el enlace siguiente:

<https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1147?title=Seguridad%20de%20la%20informaci%C3%B3n%20y%20ciberseguridad:%20nuevo%20reglamento%20para%20promover%20un%20entorno%20seguro%20y%20confiable%20en%20beneficio%20de%20los%20usuarios%20de%20los%20sistemas%20supervisados>

²⁰ El artículo 17° del Reglamento de Ciberseguridad establece que la autenticación es un proceso que debe implementarse para controlar el acceso a los servicios por canales digitales que ofrece una empresa a sus usuarios; por lo que, debe considerar: (a) Los factores de autenticación requeridos; (b) estándares criptográficos vigentes basados en software o hardware, y sus prestaciones de confidencialidad o integridad esperadas; (c) plazos y condiciones en las que se requerirá al usuario volver a autenticarse; (d) línea base de controles de seguridad de la información requerida para prevenir amenazas y (e) lineamientos para la retención de registros de auditoría para la detección de amenazas conocidas y eventos de seguridad de la información.

²¹ **RESOLUCIÓN SBS N° 504-2021, REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD, publicada el 23 de febrero de 2021 y vigente desde el 1 de julio de 2021**
Artículo 2°.- Definiciones

Para efectos de la aplicación del presente Reglamento deben considerarse las siguientes definiciones:

(...)

j) Factores de autenticación de usuario: Aquellos factores empleados para verificar la identidad de un usuario, que pueden corresponder a las siguientes categorías:

- Algo que solo el usuario conoce.
- Algo que solo el usuario posee.
- Algo que el usuario es, que incluye las características biométricas.

²² **RESOLUCIÓN SBS N° 504-2021, REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD, publicada el 23 de febrero de 2021 y vigente desde el 1 de julio de 2021**
Artículo 19. Autenticación reforzada para operaciones por canal digital

58. Adicionalmente, la SBS a través del Oficio N° 01690-2024-SBS del 11 de enero de 2024, precisó que la **autenticación reforzada** en caso se realice una operación de pago en un comercio electrónico se tiene que efectuar mediante los factores de autenticación que la entidad financiera implemente y ponga a disposición de los usuarios²³.
59. Con relación a lo que debe entenderse por canal digital²⁴ el literal d) del artículo 2° de la referida disposición legal²⁵ señala que es el medio empleado por las empresas que proveen servicios, cuyo almacenamiento, procesamiento y transmisión se realiza mediante la representación de datos en bits.
60. Por tanto, toda operación realizada por un medio que utilice datos en bits²⁶ —entendiéndose por *bits* a las unidades mínimas de información— y que cuente con un

Se requiere de autenticación reforzada para aquellas acciones que puedan originar operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente, como las operaciones a través de un canal digital que impliquen pagos o transferencia de fondos a terceros, registro de un beneficiario de confianza, modificación en los productos de seguro ahorro/inversión contratados, la contratación de un producto o servicio, modificación de límites y condiciones, para lo cual se requiere:

- Utilizar una combinación de factores de autenticación, según el literal j) del artículo 2 del presente Reglamento que, por lo menos, correspondan a dos categorías distintas y que sean independientes uno del otro.
- Generar un código de autenticación mediante métodos criptográficos, a partir de los datos específicos de cada operación, el cual debe utilizarse por única vez
- Cuando la operación sea exitosa, notificar los datos de la operación al usuario.

- ²³ En esa misma línea, mediante Oficio N° 01690-2024-SBS del 11 de enero de 2024 dirigida a la Secretaría Técnica de la Comisión, la Superintendencia de Banca, Seguros y AFP precisó los alcances del artículo 19° del Reglamento, señalando lo siguiente:

La autenticación reforzada es un requerimiento general, asociado a las condiciones específicas para cada operación que puede generar perjuicio al usuario. No obstante, existe un régimen de exención aplicable para situaciones de bajo riesgo efectuadas bajo responsabilidad de la empresa. (...)

(Subrayado nuestro)

- ²⁴ De acuerdo a la prepublicación de la norma, se señaló que el canal digital era el medio utilizado por las empresas para proveer servicios en línea, por ejemplo, teléfonos móviles, cajeros automáticos, terminales de puntos de atención, y otros cuyo almacenamiento, procesamiento y transmisión se realiza mediante la representación de datos en bits. Esta información se puede observar en el siguiente link:
<https://intranet2.sbs.gob.pe/Preproyectos/6008CQJ2FRPOCYMEEKIOW2WIXQDWEMXBYA.PDF>

- ²⁵ **RESOLUCIÓN SBS N° 504-2021, REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD, publicada el 23 de febrero de 2021 y vigente desde el 1 de julio de 2021**

Artículo 2°. – Definiciones

Para efectos de la aplicación del presente Reglamento deben considerarse las siguientes definiciones:

(...)

- Canal digital:** Medio empleado por las empresas para proveer servicios cuyo almacenamiento, procesamiento y transmisión se realiza mediante la representación de datos en bits.

- ²⁶ El departamento de Ciencias e Ingeniería de la Computación de la Universidad Nacional del Sur – Bahía Blanca señala que las medidas de almacenamiento son importantes porque permiten verificar la capacidad de almacenamiento de los dispositivos, así indican que la información que se almacena en un dispositivo se representa en forma binaria, precisando que el Bit es la mínima unidad de información. Esta información se puede observar en el siguiente enlace:
<https://cs.uns.edu.ar/materias/iocp/downloads/Clases%20Teoricas/Clase-01-Conceptos-basicos-Hardware.pdf>

En la misma línea, el Instituto de Ingeniería de la Universidad Nacional Autónoma de México señala que las computadoras emplean velocidades de procesamiento y *capacidades de almacenamiento como el bit*, siendo que solo puede contener dos valores: cero y uno, además, señalan que existen unidades de medición que recogen el concepto de bit, por ejemplo, bps (bits por segundo), entre otros. Así, se puede verificar en el siguiente enlace <https://www.iingen.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/debitsydebytes.aspx>

circuito de almacenamiento, procesamiento y transmisión donde la información se represente en dicha medida, será considerada como una operación efectuada por canal digital.

61. Ello, va en la misma línea de lo indicado por la SBS, a través del Oficio N° 01690-2024-SBS del 11 de enero de 2024, al considerar que los canales; tales como, comercios electrónicos, y *point of sale* (POS), cajeros automáticos y similares, a través de los cuales las entidades financieras proveen sus servicios a los usuarios, deberán ser considerados como canales digitales, en lo que concierne a dichos servicios²⁷
62. Cabe precisar que, las acciones que puedan generar operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente, engloba además de las indicadas en el artículo 19° de la norma -según la SBS- los aplicativos móviles, la banca por internet, las billeteras digitales, los cajeros automáticos (ATM) y los terminales de punto de venta (POS), así como las operaciones de comercio electrónico que utilicen instrumentos de pago provistos por las entidades²⁸, es decir, se contemplan los siguientes supuestos:

Cuadro N°1: Supuestos establecidos en la norma

Supuestos establecidos en la normativa	
Acciones que puedan generar operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente	Operaciones que impliquen pagos a terceros
	Operaciones a que impliquen transferencia de fondos a terceros
	Operaciones que se realicen por aplicativos móviles
	Operaciones realizadas por la banca por internet
	Operaciones realizadas a través de billeteras digitales
	Operaciones realizadas en cajeros automáticos (ATM)
	Operaciones realizadas en terminales de punto de venta (POS)
Operaciones de comercio electrónico que utilicen instrumentos de pago provistos por las entidades	

Asimismo, de la publicación denominada "Claude Shannon, el olvidado inventor de la era digital" del 31 de abril de 2021 realizado por el Banco BBVA, manifestó que el *bit* (*binary digit*) es un término acuñado por John Tukey, quien propuso que toda información, sea en lengua escritos, oral, imágenes o vídeos, podía ser digitalizada; es decir, podía ser materializada en bits. Dicha información se puede visualizar en el siguiente enlace: <https://www.bbvaopenmind.com/tecnologia/visionarios/claude-shannon-inventor-de-la-era-digital/>

En atención a los argumentos señalados, se puede concluir que el bit es la unidad mínima de información y es utilizada como medida de información en diversos ámbitos.

²⁷ En esa misma línea, mediante Oficio N° 01690-2024-SBS del 11 de enero de 2024 dirigida a la Secretaría Técnica de la Comisión, la Superintendencia de Banca, Seguros y AFP precisó los alcances del artículo 2° del Reglamento, señalando lo siguiente:

"El Reglamento establece lineamientos de carácter general que las entidades financieras deben implementar según el contexto particular de su operación, y no tiene por finalidad establecer una lista limitativa de canales considerados digitales o de describir todas las formas posibles de implementación."

Canal digital

El literal d) del Artículo 2° del Reglamento, establece que un canal digital es cualquier medio empleado por las empresas supervisadas para proveer servicios, cuyo almacenamiento, procesamiento y transmisión se realiza mediante la representación de datos en bits.

En ese sentido, los canales como comercios electrónicos, POS, cajeros automáticos y similares, a través de los cuales las entidades financieras proveen sus servicios a los usuarios, son considerados canales digitales, en lo que concierne a dichos servicios, en la medida que cumplen con la definición mencionada anteriormente.

(Subrayado nuestro)

²⁸ Ver la información detallada en el Boletín Semanal SBS Informa N° 24 de julio de 2022, "Autenticación reforzada: mayor seguridad para operaciones que puedan generar perjuicio al usuario", en el siguiente enlace: <https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1222>

	Registro de un beneficiario de confianza
	Modificación en los productos de seguro, ahorro/inversión contratados
	Contratación de un producto o servicio
	Modificación de límites y condiciones
	Otros

63. Ahora bien, de conformidad con lo establecido por el artículo 19° concordado con el artículo 2, literal j) del Reglamento del Ciberseguridad, para que exista autenticación reforzada se requerirá cumplir con lo siguiente:

- a) Utilizar una combinación de factores de autenticación que, por lo menos, correspondan a dos categorías distintas y que sean independientes uno del otro. Cabe precisar que, la SBS explicó las categorías de dichos factores; asimismo, brindó algunos ejemplos²⁹, conforme a lo que se detalla a continuación:
 - (i) **Algo que el usuario conoce:** contraseña, PIN, respuestas de preguntas clave, entre otros.
 - (ii) **Algo que el usuario posee:** certificado digital, token físico o de *software*, clave dinámica, entre otros.
 - (iii) **Algo que el usuario es:** huella digital, patrón de iris, reconocimiento facial, entre otros.
- b) Generar un código de autenticación mediante métodos criptográficos, a partir de los datos específicos de cada operación, el cual debe utilizarse por única vez.
- c) Cuando la operación sea exitosa, notificar los datos de la operación al usuario.

64. Así, conforme a lo señalado, se entenderá que el proveedor ha cumplido con aplicar la autenticación reforzada cuando demuestre haber efectuado los pasos antes señalados.

65. Por otro lado, con relación a la notificación de los datos de la operación al usuario, debe indicarse que la misma implica que el usuario pueda tomar conocimiento oportunamente de las transacciones fraudulentas y comunicarlas a la entidad financiera, a fin de que adopte las acciones para evitar que se efectúen nuevas operaciones. Cabe precisar que, pueden emplearse mecanismos de notificación alternativos al correo electrónico o mensaje de texto (SMS), siempre que tenga un propósito similar al requerimiento en la disposición legal³⁰.

²⁹ Ver la información detallada en el Boletín Semanal SBS Informa N° 16 de mayo de 2021, "Seguridad de la información y ciberseguridad: fortaleciendo los procesos de autenticación en beneficio de los usuarios de los sistemas supervisados", en el siguiente enlace:

<https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1157?title=Seguridad%20de%20la%20informaci%C3%B3n%20y%20ciberseguridad:%20fortaleciendo%20los%20procesos%20de%20autenticaci%C3%B3n%20en%20beneficio%20de%20los%20usuarios%20de%20los%20sistemas%20supervisados>

³⁰ Ver la información detallada en el Boletín Semanal SBS Informa N° 24 de julio de 2022, "Autenticación reforzada: mayor seguridad para operaciones que puedan generar perjuicio al usuario", en el siguiente enlace: <https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1222>

66. Asimismo, la SBS señala, a modo de ejemplo, las siguientes consideraciones sobre los factores de autenticación³¹:
- (i) El número de DNI no constituye un factor de autenticación de conocimiento admisible; y, si se utiliza el reconocimiento del DNI como factor de autenticación que solo el usuario posee, la entidad debe demostrar con evidencia razonable el éxito de autenticación del uso de este factor;
 - (ii) el CVV, número de tarjeta, nombre del titular y fecha de vencimiento, cuando estén contenidos en la tarjeta, constituyen un único factor de autenticación que demuestra la posesión de esta, por lo que se debe complementar con otro factor para aplicar la autenticación reforzada;
 - (iii) la contraseña de un solo uso (OTP) enviada mediante mensaje SMS no es considerada como un factor de autenticación válido, pues su transmisión no es segura y expone a los usuarios a incidentes de seguridad de la información;
 - (iv) las alternativas seguras que pueden considerarse como un factor de autenticación de posesión son las notificaciones *push* y el uso de tokens digitales; y,
 - (v) respecto al uso de factores de autenticación biométricos, como el escaneo de la huella digital o del rostro, las entidades preverán el uso de tecnologías con alto ratio de fiabilidad, donde se minimicen falsos positivos y falsos negativos.
67. Adicionalmente, el artículo 20 del Reglamento de Ciberseguridad³², como excepción a la aplicación de lo indicado en el literal c) del artículo 19 de la referida disposición legal, describe exenciones a la autenticación reforzada, entre las cuales se encuentran:

³¹ Ver la información detallada en el Boletín Semanal SBS Informa N° 24 de julio de 2022, "Autenticación reforzada: mayor seguridad para operaciones que puedan generar perjuicio al usuario", en el siguiente enlace: <https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1222>

³² **RESOLUCIÓN SBS N° 504-2021, REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD, publicada el 23 de febrero de 2021, modificada mediante Resolución SBS N° 03240-2023, publicada el 3 de octubre de 2023 y vigente, en este artículo, desde el 4 de octubre de 2023**

Artículo 20. Exenciones de autenticación reforzada para operaciones por canal digital

20.1 Están exentas del requisito de autenticación reforzada indicado en el artículo 19 del presente Reglamento, a excepción del indicado en el literal c), las siguientes operaciones realizadas por canal digital:

a) Las operaciones de pago, pagos periódicos o transferencia hacia un beneficiario registrado previamente por el usuario como beneficiario de confianza, como destinatario usual de dichas operaciones.

b) Las operaciones de pago, pagos periódicos o transferencias a cuentas en las que el cliente y el beneficiario sean la misma persona, sea natural o jurídica, y siempre que dichas cuentas se mantengan en la misma empresa.

20.2 Las operaciones de pago y transferencia que presenten un nivel de riesgo de fraude bajo, como resultado de un análisis del riesgo en línea por operación, están exentas de la autenticación reforzada, siempre que la empresa cumpla con:

i. Implementar alguno de los estándares de la industria de pagos, EMV 3DS y tokenización de pagos EMV, en sus versiones más recientes.

ii. Definir el monto de umbral por operación por debajo del cual aplicará la exención por el citado análisis de riesgos.

iii. Medir periódicamente el ratio de fraude de las operaciones de pago por canal y tipo de operación.

iv. Actualizar periódicamente las reglas aplicables en el análisis de riesgo en función al indicador de riesgo de fraude.

v. Utilizar los datos que estén disponibles por cada tipo de operación, que incluye, pero no se limita a, los asociados al comportamiento del usuario, al medio utilizado y los que de este se pueda obtener para fines del análisis de riesgo.

20.3 Las operaciones no reconocidas por los clientes que hayan sido efectuadas en aplicación de la exención señalada en el párrafo 20.2 del presente artículo, o que fueron realizadas luego de que el usuario reportara el robo o pérdida de sus credenciales, son responsabilidad de la empresa, para lo cual deben implementar mecanismos que ante el repudio de la operación por parte del usuario garanticen su aplicación inmediata.

- (i) Las operaciones de pago realizadas a un beneficiario, el cual está registrado como usuario de confianza, como destinatario usual de dichas operaciones;
- (ii) operaciones de pago realizadas entre cuentas donde el cliente y el beneficiario sean la misma persona, además, dichas cuentas deben pertenecer a la misma empresa; y,
- (iii) operaciones de pago y transferencias realizadas debajo del umbral por operación establecido por la empresa, entre otros requerimientos.

68. Para una mayor comprensión de lo expuesto en los numerales precedentes, se inserta a continuación un gráfico explicativo de los requisitos exigibles para la realización de una operación con autenticación reforzada:

Gráfico N° 1: Requisitos exigibles para la autenticación reforzada

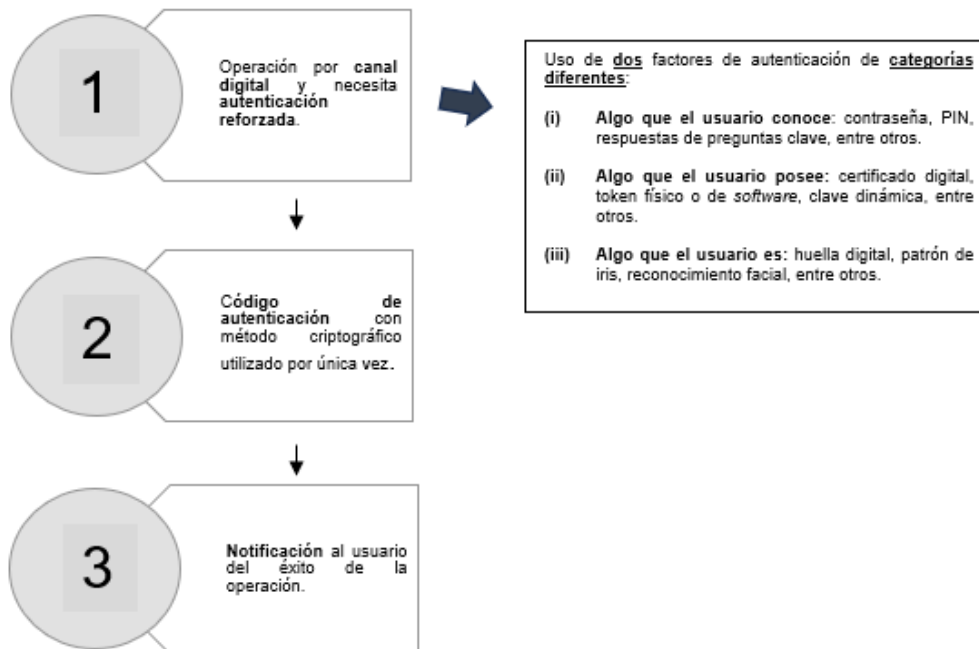


Gráfico elaborado por la Secretaría Técnica de la Comisión de Protección al Consumidor N° 1

69. En virtud a lo expuesto, y conforme a lo establecido en el Reglamento de Ciberseguridad, para operaciones realizadas desde el 2 de julio de 2022, la norma exige a las empresas supervisadas de Régimen General y Régimen Simplificado una autenticación reforzada, a fin de garantizar que los usuarios realicen operaciones por canales digitales en un entorno seguro y evitar situaciones que generen un abuso del servicio en perjuicio del cliente.
70. Por ello, ante el cuestionamiento de un consumidor, la entidad debe estar en la posibilidad de acreditar de manera suficiente y fehaciente que la operación cargada ha sido debidamente autorizada por este, conforme a lo establecido en el Reglamento de Ciberseguridad, lo cual será analizado a partir de los medios probatorios que obran en

el expediente; ello en el marco de una adecuada gestión de los riesgos asociados a la seguridad de las operaciones realizadas por canal digital autorizadas por las empresas del sistema financiero.

— **Sobre la presunta responsabilidad de Banco al permitir la realización de las operaciones no reconocidas**

71. En el presente caso, el OPS declaró infundada la denuncia interpuesta por la señora Arbe contra el Banco, en la medida que se había configurado la ruptura del nexo causal para la realización de la operación materia de denuncia, la cual se detalla a continuación:

Fecha	Detalle	Importe S/
14/07/2023	TRANSF. BCO. SCOTIA B	5 240,80

72. En su apelación, la señora Arbe señaló que aun cuando el OPS hubiese señalado que se había configurado la ruptura del nexo causal, lo cierto era que el proveedor denunciado no había cumplido con las medidas de seguridad dispuestas por la normativa sectorial aplicable.

73. Así, teniendo en consideración que la operación cuestionada se efectuó a través del aplicativo móvil del Banco en el mes de julio de 2023, esto es, con posterioridad a la entrada en vigencia del Reglamento de Ciberseguridad, a fin de determinar la responsabilidad de la entidad bancaria, corresponde analizar si la operación no reconocida por el denunciante por la denunciante se efectuó con una autenticación reforzada, la cual consta de (a) una combinación de factores de autenticación, (b) la generación de un código de autenticación mediante métodos criptográficos con los datos específicos de cada operación, el cual debe ser utilizado una sola vez; y, (c) la notificación al usuario sobre la operación una vez que se efectúe con éxito.

74. Sobre este punto, conforme se señaló en los antecedentes de la presente resolución, mediante Resolución N° 2 del 10 de abril de 2024, la Secretaría Técnica formuló un requerimiento al Banco, en atención a la aplicación del Reglamento de Ciberseguridad.

75. Cabe precisar que el requerimiento fue absuelto parcialmente por el Banco, cuestionando la competencia del Indecopi para requerir información vinculada a las medidas de ciberseguridad, alegación que ha sido previamente desvirtuada.

(i).1 De la validez de las operaciones materia de denuncia

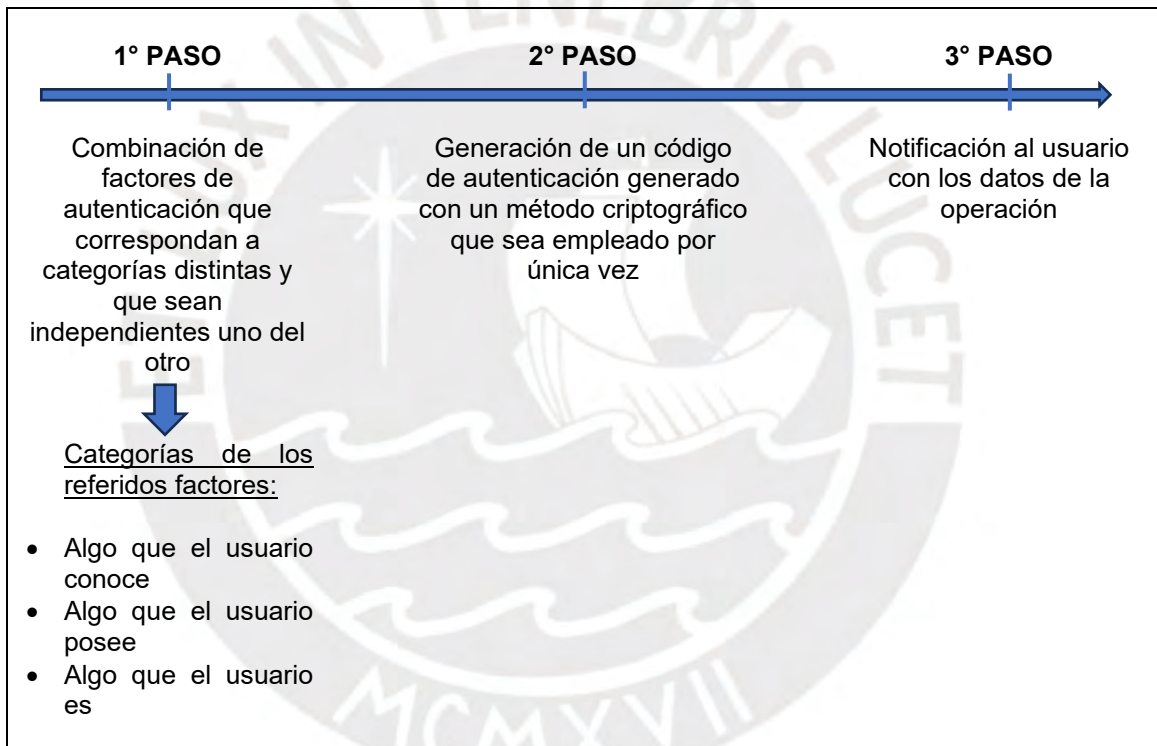
a) Sobre el enrolamiento

76. Con relación al enrolamiento requerido para la realización de operaciones mediante canales digitales, este Colegiado debe indicar que ello no ha sido cuestionado por la señora Arbe, por lo que no corresponde analizar su enrolamiento a los servicios brindados por el Banco a través de canales digitales.

77. Dicho esto, se procederá a verificar si el Banco ha ofrecido medios probatorios que permiten verificar la observancia de las disposiciones del Reglamento de Ciberseguridad, relacionadas con la aplicación de autenticación reforzada.

b) Sobre la autenticación reforzada

78. Respecto a este punto corresponde señalar que, mediante la Resolución N° 2 del 10 de abril de 2024, se efectuó un requerimiento de información al Banco respecto a la aplicación del Reglamento de Ciberseguridad; sin embargo, dicho requerimiento fue atendido de manera parcial.
79. Ahora bien, respecto de la autenticación reforzada, el artículo 19° del Reglamento de Ciberseguridad dispone que se deben emplear tres (3) pasos o requisitos cuyo cumplimiento se analizará en los numerales siguientes. Así, para una mejor comprensión, se ha elaborado el siguiente gráfico:

Gráfico N° 1: Tres (3) pasos que conforman la autenticación reforzada

80. Respecto del primer paso, referido a la utilización de una combinación de factores de autenticación que correspondan a categorías distintas y que sean independientes uno del otro, como algo que el usuario conoce (contraseña, el PIN, respuestas a preguntas claves, entre otros), algo que el usuario posee (la clave dinámica) y, algo que el usuario es (huella digital, patrón de iris, reconocimiento facial, entre otros), el Banco se la limitado a indicar que el Indecopi no es la autoridad competente para verificar el cumplimiento de las medidas de ciberseguridad.
81. El argumento del Banco ha sido desvirtuado en la cuestión previa de la presente resolución, pues el Indecopi cuenta con facultades para determinar el cumplimiento de

dichas medidas, siendo que en el presente caso no es posible verificar ello. Es pertinente precisar que si bien en los descargos que obran en el expediente, el proveedor denunciado ha indicado que la operación se realizó en estricto cumplimiento de sus medidas de seguridad (empleando la clave token, así como la clave de seis dígitos), lo cierto es que no ha explicado como es que dichos elementos coinciden con los factores del Reglamento de Ciberseguridad.

82. Por otra parte, respecto al segundo paso, el Banco ha señalado que la clave token es el código de autenticación generado con un método criptográfico que ha sido empleado por única vez, el cual además se genera a partir de una semilla criptográfica que impide que sea adivinado o calculado por el consumidor.
83. Al respecto, se reitera que el artículo 19° del Reglamento de Ciberseguridad dispone que el segundo paso consiste en la generación de un código de autenticación mediante métodos criptográficos, a partir de los datos específicos de cada operación.
84. Esto quiere decir que una vez que se efectúe la operación, los datos de esta permitirán que se origine el código de autenticación mediante métodos criptográficos, no siendo posible que el referido código de autenticación pueda consistir en un elemento que forma parte del proceso de realización de la operación (como lo es la clave token), puesto que el segundo paso es consecuencia de la validación de los factores de autenticación que permitieron que la operación se concrete.
85. Dicho esto, corresponde señalar que, en conformidad con el artículo 19° del Reglamento de Ciberseguridad, a criterio de este Colegiado, el clave token no puede ser considerada como el segundo paso.
86. Respecto del tercer paso, el Banco ha presentado su reporte denominado "Constancia", el cual evidenciaría que se notificó a la denunciante sobre la válida realización de la operación. Sin embargo, dicho medio probatorio no contiene elemento alguno que permita evidenciar que fue enviado y recibido por la señora Arbe.
87. Por lo expuesto, esta Comisión puede concluir que el Banco no ha cumplido con acreditar el empleo de todas las medidas de seguridad contempladas en el Reglamento de Ciberseguridad, pese a que ello le ha sido requerido mediante Resolución N° 2 del 10 de abril de 2024.
88. Por consiguiente, del análisis efectuado, se desprende el Banco permitió que se realice de forma inválida una operación no reconocida con cargo a la cuenta de ahorros de la denunciante, puesto que no ha acreditado que esta se efectuó con observancia de las medidas de seguridad dispuestas en el Reglamento de Ciberseguridad.
89. Sin perjuicio de lo antes mencionado, en tanto la señora Arbe denunció que las operaciones no reconocidas no corresponderían a su comportamiento habitual de consumo, se procederá a analizarlas a fin de determinar ello.

(i).2 Del comportamiento habitual de la denunciante

90. Como bien se ha señalado, las entidades del sistema financiero se encuentran obligadas por la norma a contar con sistemas de monitoreo que les permitan detectar operaciones

que no correspondan al comportamiento habitual de cada consumidor o que obedezcan a patrones de fraude. El funcionamiento del sistema de monitoreo es definido por las reglas que cada entidad financiera establezca, conforme al análisis del tipo de consumos que se realicen con las tarjetas de crédito y débito que administran.

91. Ahora bien, en lo que respecta a la generación de alertas, para que estas se efectúen deben concurrir circunstancias suficientes para inferir que una operación no está siendo realizada por el titular de la cuenta de ahorros y/o tarjeta de crédito.
92. En ese sentido, deben concurrir varios elementos que puedan calificarse como inusuales y, en consecuencia, generar la alerta en el sistema de la entidad bancaria.
93. Asimismo, es importante añadir que para que el sistema de monitoreo pueda activar una alerta, primero deben haberse realizado operaciones que permitan a este presumir que no están siendo realizadas por el titular de la tarjeta, pues no es posible que el sistema se active antes de la realización de las operaciones que contienen características de patrón de fraude o sean distintas al comportamiento habitual del consumidor.
94. Por lo que, primero corresponde verificar, conforme al funcionamiento del sistema de monitoreo y los medios aportados durante el procedimiento, si las operaciones cuestionadas debieron generar una alerta en el sistema del Banco; para luego, analizar si la entidad financiera cumplió con esta obligación de manera debida
95. Cabe señalar que a través de su escrito de descargos, el Banco indicó que al ser una única operación, su sistema de monitorio no pudo haberla considerado como inusual, por lo que no había indicios que ameritasen la generación de alertas.
96. Ahora bien, en tanto la operación materia de denuncia resultó ser la primera operación cuestionada, contrariamente a lo alegado por la señora Arbe en su escrito de denuncia, no era posible para el sistema de monitoreo del Banco efectuar un bloqueo de manera previa, en la medida que, tal como se ha indicado precedentemente, se requería del proceso de dicha transacción para que esta pueda ser analizada por los sistemas de monitoreo de la entidad bancaria:
97. Por lo tanto, la Comisión considera que no ha quedado acreditado que el Banco haya incumplido con las medidas de seguridad sobre el sistema de monitoreo; en tanto la operación de S/ 5 240,80, constituye la primera operación realizada con cargo a la cuenta de ahorros de la denunciante.
98. Habiendo efectuado el análisis correspondiente, se verifica lo siguiente:
 - (i) El Banco no adoptó las medidas de seguridad pertinentes al permitir que se efectúe una (1) operación con cargo a la cuenta de ahorros de la denunciante; toda vez que ha quedado que no se efectuó válidamente; y,
 - (ii) no correspondía que el Banco activara su sistema de monitoreo pues la operación materia de denuncia era la única operación que fue realizada con cargo a la cuenta de ahorros de la denunciante.

(i).3 Conclusión

99. Por las consideraciones expuestas, este Colegiado considera que corresponde revocar la Resolución Final N° 1881-2023/PS2, en el extremo que declaró infundada la denuncia interpuesta por la señora Arbe contra el Banco por presunta infracción a los artículos 1° literal c), 18° y 19° del Código; y, reformándola, declarar fundada la denuncia, en la medida que se ha verificado que la entidad bancaria no adoptó las medidas de seguridad pertinentes, al permitir que se debite indebidamente una operación en la Cuenta de Ahorros N° 191-*****0-80 de la denunciante, la cual correspondía a su patrón habitual de consumo, de acuerdo con el siguiente detalle:

FECHA	DETALLE	IMPORTE S/
14/07/2023	TRANSF. BCO. SCOTIA B	5 204,80

Sobre las medidas correctivas

100. El artículo 114° del Código establece que, sin perjuicio de la sanción administrativa que corresponda al proveedor por una infracción a las normas del Código, el Indecopi puede dictar, en calidad de mandatos, medidas correctivas reparadoras y complementarias³³.
101. Las medidas correctivas reparadoras tienen el objeto de resarcir las consecuencias patrimoniales directas e inmediatas ocasionadas al consumidor por la infracción administrativa a su estado anterior³⁴. Las medidas correctivas complementarias tienen

³³ **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de setiembre de 2010**
Artículo 114.- Medidas correctivas
Sin perjuicio de la sanción administrativa que corresponda al proveedor por una infracción al presente Código, el Indecopi puede dictar, en calidad de mandatos, medidas correctivas reparadoras y complementarias.
Las medidas correctivas reparadoras pueden dictarse a pedido de parte o de oficio, siempre y cuando sean expresamente informadas sobre esa posibilidad en la notificación de cargo al proveedor por la autoridad encargada del procedimiento. Las medidas correctivas complementarias pueden dictarse de oficio o a pedido de parte.

³⁴ **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de setiembre de 2010**
Artículo 115.- Medidas correctivas reparadoras
115.1 Las medidas correctivas reparadoras tienen el objeto de resarcir las consecuencias patrimoniales directas e inmediatas ocasionadas al consumidor por la infracción administrativa a su estado anterior. En caso el órgano resolutorio dicte una o varias medidas correctivas, debe considerar lo acordado por las partes durante la relación de consumo. Las medidas correctivas reparadoras pueden consistir en ordenar al proveedor infractor lo siguiente:
a. Reparar productos.
b. Cambiar productos por otros de idénticas o similares características, cuando la reparación no sea posible o no resulte razonable según las circunstancias.
c. Entregar un producto de idénticas características o, cuando esto no resulte posible, de similares características, en los supuestos de pérdida o deterioro atribuible al proveedor y siempre que exista interés del consumidor.
d. Cumplir con ejecutar la prestación u obligación asumida; y si esto no resulte posible o no sea razonable, otra de efectos equivalentes, incluyendo prestaciones dinerarias.
e. Cumplir con ejecutar otras prestaciones u obligaciones legales o convencionales a su cargo.
f. Devolver la contraprestación pagada por el consumidor, más los intereses legales correspondientes, cuando la reparación, reposición, o cumplimiento de la prestación u obligación, según sea el caso, no resulte posible o no sea razonable según las circunstancias.
g. En los supuestos de pagos indebidos o en exceso, devolver estos montos, más los intereses correspondientes.
h. Pagar los gastos incurridos por el consumidor para mitigar las consecuencias de la infracción administrativa.
i. Otras medidas reparadoras análogas de efectos equivalentes a las anteriores.
115.2 Las medidas correctivas reparadoras no pueden ser solicitadas de manera acumulativa conjunta, pudiendo plantearse de manera alternativa o subsidiaria, con excepción de la medida correctiva señalada en el literal h) que puede solicitarse conjuntamente con otra medida correctiva. Cuando los órganos competentes del Indecopi se pronuncian respecto de una medida correctiva reparadora, aplican el principio de congruencia procesal.
115.3 Las medidas correctivas reparadoras pueden solicitarse en cualquier momento hasta antes de la notificación de cargo al proveedor, sin perjuicio de la facultad de secretaría técnica de la comisión de requerir al consumidor que precise la medida correctiva materia de solicitud. El consumidor puede variar su solicitud de medida correctiva

el objeto de revertir los efectos de la conducta infractora o evitar que se produzca nuevamente en el futuro³⁵.

102. En el presente caso, ha quedado acreditado que el Banco no adoptó las medidas de seguridad pertinentes, al permitir que se debite indebidamente una operación en la Cuenta de Ahorros N° 191-*****0-80 de la denunciante, la cual correspondía a su patrón habitual de consumo.
103. Por tanto, este Colegiado considera que corresponde ordenar al Banco, en calidad de medida correctiva, que en un plazo no mayor de quince (15) días hábiles contado a partir del día siguiente de la notificación de la presente resolución, cumpla con restituir en la Cuenta de Ahorros N° 191-*****0-80 el importe de la operación no reconocida declarada fundada en la presente resolución, así como los intereses dejados de percibir por dicho monto, calculados para el periodo comprendido entre a fecha de realización de la operación y la fecha efectiva de extorno, empleando la tasa de rendimiento correspondiente a dicha cuenta.
104. Asimismo, en un plazo no mayor de cinco (5) días hábiles contado a partir del vencimiento del plazo mencionado en el párrafo anterior, el Banco deberá presentar ante el OPS los medios probatorios que acrediten el cumplimiento del mandato

hasta antes de la decisión de primera instancia, en cuyo caso se confiere traslado al proveedor para que formule su descargo.

- 115.4 Corresponde al consumidor que solicita el dictado de la medida correctiva reparadora probar las consecuencias patrimoniales directas e inmediatas causadas por la comisión de la infracción administrativa.
- 115.5 Los bienes o montos objeto de medidas correctivas reparadoras son entregados por el proveedor directamente al consumidor que los reclama, salvo mandato distinto contenido en la resolución. Aquellos bienes o montos materia de una medida correctiva reparadora, que por algún motivo se encuentran en posesión del Indecopi y deban ser entregados a los consumidores beneficiados, son puestos a disposición de estos.
- 115.6 El extremo de la resolución final que ordena el cumplimiento de una medida correctiva reparadora a favor del consumidor constituye título ejecutivo conforme con lo dispuesto en el artículo 688 del Código Procesal Civil, una vez que quedan consentidas o causan estado en la vía administrativa. La legitimidad para obrar en los procesos civiles de ejecución corresponde a los consumidores beneficiados con la medida correctiva reparadora.
- 115.7 Las medidas correctivas reparadoras como mandatos dirigidos a resarcir las consecuencias patrimoniales directas e inmediatas originadas por la infracción buscan corregir la conducta infractora y no tienen naturaleza indemnizatoria; son dictadas sin perjuicio de la indemnización por los daños y perjuicios que el consumidor puede solicitar en la vía judicial o arbitral correspondiente. No obstante, se descuenta de la indemnización patrimonial aquella satisfacción patrimonial deducible que el consumidor haya recibido a consecuencia del dictado de una medida correctiva reparadora en sede administrativa.

³⁵

LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de setiembre de 2010
Artículo 116.- Medidas correctivas complementarias

Las medidas correctivas complementarias tienen el objeto de revertir los efectos de la conducta infractora o evitar que esta se produzca nuevamente en el futuro y pueden ser, entre otras, las siguientes:

- a. Que el proveedor cumpla con atender la solicitud de información requerida por el consumidor, siempre que dicho requerimiento guarde relación con el producto adquirido o servicio contratado.
- b. Declarar inexigibles las cláusulas que han sido identificadas como abusivas en el procedimiento.
- c. El decomiso y destrucción de la mercadería, envases, envolturas o etiquetas.
- d. En caso de infracciones muy graves y de reincidencia o reiterancia:
 - (i) Solicitar a la autoridad correspondiente la clausura temporal del establecimiento industrial, comercial o de servicios por un plazo máximo de seis (6) meses.
 - (ii) Solicitar a la autoridad competente la inhabilitación, temporal o permanente, del proveedor en función de los alcances de la infracción sancionada.
- e. Publicación de avisos rectificatorios o informativos en la forma que determine el Indecopi, tomando en consideración los medios que resulten idóneos para revertir los efectos que el acto objeto de sanción ha ocasionado.
- f. Cualquier otra medida correctiva que tenga el objeto de revertir los efectos de la conducta infractora o evitar que esta se produzca nuevamente en el futuro.

El Indecopi está facultado para solicitar a la autoridad municipal y policial el apoyo respectivo para la ejecución de las medidas correctivas complementarias correspondientes.

ordenado, bajo apercibimiento de imponer una multa coercitiva conforme a lo establecido en el artículo 117 del Código³⁶.

105. En este punto, cabe indicar que el artículo 40 de la Directiva señala que, si se produce el incumplimiento del mandato por parte del proveedor obligado, la autoridad administrativa, a fin de garantizar el cumplimiento de su decisión, actuará de oficio e impondrá multa coercitiva por incumplimiento de medida correctiva³⁷.
106. Cabe precisar que no constituye una facultad del Indecopi ejecutar la medida correctiva a favor del consumidor, pues el Estado ha reservado esta potestad únicamente al consumidor mediante la vía judicial. Por estas razones, el numeral 115.6 del artículo 115 del Código establece que las resoluciones finales que ordenen medidas correctivas reparadoras constituyen Títulos de Ejecución conforme a lo dispuesto en el artículo 688 del Código Procesal Civil.

Sobre la graduación de la sanción

107. El 14 de junio de 2021³⁸, entró en vigencia el Decreto Supremo N° 032-2021-PCM, Decreto Supremo que aprueba la graduación, metodología y factores para la

³⁶ **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de setiembre de 2010 y modificada por el Decreto Legislativo 1308, publicado el 30 de diciembre de 2016**

Artículo 117.- Multas coercitivas por incumplimiento de mandatos

Si el obligado a cumplir con un mandato del Indecopi respecto a una medida correctiva o a una medida cautelar no lo hace, se le impone una multa coercitiva no menor de una (1) Unidad Impositiva Tributaria, tratándose de una microempresa; en todos los otros supuestos se impone una multa no menor de tres (3) Unidades Impositivas Tributarias (UIT).

En caso de persistir el incumplimiento de cualquiera de los mandatos a que se refiere el primer párrafo, el órgano resolutorio puede imponer una nueva multa, duplicando sucesivamente el monto de la última multa impuesta hasta el límite de doscientas (200) Unidades Impositivas Tributarias (UIT). La multa que corresponda debe ser pagada dentro del plazo de cinco (5) días hábiles, vencido el cual se ordena su cobranza coactiva.

No cabe la impugnación de las multas coercitivas previstas en el presente artículo.
(Subrayado agregado)

³⁷ **DIRECTIVA N° 001-2021/DIR-COD-INDECOPI, DIRECTIVA ÚNICA QUE REGULA LOS PROCEDIMIENTOS DE PROTECCIÓN AL CONSUMIDOR PREVISTOS EN EL CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR Ejecución de Mandatos**

Artículo 40.- Incumplimiento y ejecución de medidas correctivas o cautelares

40.1. Ante el incumplimiento de un mandato de medida correctiva o medida cautelar por el proveedor obligado, el órgano resolutorio que actúa como primera instancia en el procedimiento, debe actuar de oficio a fin de garantizar el cumplimiento de la decisión de la autoridad, sin perjuicio del derecho que tiene al administrado de comunicarle esa situación. En dicha comunicación, el beneficiado debe precisar el número de expediente y resolución que dispuso el mandato, además de especificar en qué consiste el incumplimiento en caso se trate de varios mandatos.

40.2 En caso el obligado no acredite el cumplimiento de algún mandato de medida correctiva o medida cautelar, el órgano resolutorio que actúa como primera instancia, atendiendo a las circunstancias del caso, podrá otorgar al administrado obligado por el mandato un plazo adicional de dos (2) días hábiles para cumplir con el apercibimiento de comunicar el cumplimiento del mandato impuesto.

40.3. En caso el obligado no acredite el cumplimiento del mandato o se verifique el incumplimiento de la medida impuesta, el órgano resolutorio procede con la imposición de la multa coercitiva, de conformidad con lo dispuesto en el artículo 117 del Código.

40.4 En aquellos casos en que el obligado apercibido acredite el cumplimiento del mandato, el órgano resolutorio debe comunicar tal hecho al beneficiado, quien, de considerar que persiste el incumplimiento, podrá solicitar el inicio de un procedimiento en vía de ejecución por incumplimiento de medidas correctivas o cautelares, previsto en el artículo 106 del Código, debiendo cumplir con realizar el pago del derecho de tramitación, conforme a lo establecido en el Texto Único de Procedimientos Administrativos del INDECOPI.

³⁸ **DECRETO SUPREMO 032-2021-PCM, DECRETO SUPREMO QUE APRUEBA LA GRADUACIÓN, METODOLOGÍA Y FACTORES PARA LA DETERMINACIÓN DE LAS MULTAS QUE IMPONGAN LOS ÓRGANOS RESOLUTIVOS**

determinación de las multas que impongan los órganos resolutivos del INDECOPI respecto de las infracciones sancionables en el ámbito de su competencia (en adelante, Decreto Supremo N° 032-2021-PCM)³⁹, aplicable para los procedimientos administrativos de protección al consumidor a cargo de esta Comisión, en la vía ordinaria y en la vía sumarísima —como segunda instancia, a través de un recurso de apelación—, que hayan iniciado a partir de dicha fecha⁴⁰.

DEL INDECOPI RESPECTO DE LAS INFRACCIONES SANCIONABLES EN EL ÁMBITO DE SU COMPETENCIA, publicado en el Diario Oficial El Peruano el 25 de febrero de 2021.

Artículo 3. Vigencia

El presente decreto supremo entra en vigencia de manera conjunta con la entrada en vigencia de la Ley N° 31112, Ley que establece el control previo de operaciones de concentración empresarial.

LEY N° 31112, LEY QUE ESTABLECE EL CONTROL PREVIO DE OPERACIONES DE CONCENTRACIÓN EMPRESARIAL, publicada el 7 de enero de 2021

DISPOSICIONES COMPLEMENTARIAS FINALES

DUODÉCIMA. Vigencia

La presente ley entra en vigencia a los quince (15) días calendario contados a partir de la adecuación normativa establecida en la novena disposición complementaria final.

NOVENA. Adecuación

En un plazo no mayor a quince (15) días contados a partir de la publicación del reglamento de la presente ley, se dictan las modificaciones al Reglamento de la Ley de Organización y Funciones del INDECOPI y demás instrumentos de gestión de la entidad, a fin de adecuarlos a lo dispuesto por la presente ley.

DECRETO SUPREMO N° 104-2021-PCM, DECRETO SUPREMO QUE APRUEBA LA SECCIÓN PRIMERA DEL REGLAMENTO DE ORGANIZACIÓN Y FUNCIONES DEL INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL, publicado el 27 de mayo de 2021

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA.- Vigencia de la Primera Sección del Reglamento de Organización y Funciones

La Sección Primera del Reglamento de Organización y Funciones del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, aprobada por el presente Decreto Supremo, entra en vigencia a partir del día siguiente de la publicación de la Resolución que aprueba la Sección Segunda de dicho Reglamento, con excepción de la Segunda y Quinta Disposición Complementaria Final, que entran en vigencia al día siguiente de la publicación de la presente norma.

RESOLUCIÓN N° 000060-2021-PRE-INDECOPI, APRUEBAN SECCIÓN SEGUNDA DEL REGLAMENTO DE ORGANIZACIÓN Y FUNCIONES DEL INDECOPI, publicada el 30 de mayo de 2021

Artículo 1.- Aprobación de la Sección Segunda del Reglamento de Organización y Funciones del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)

Apruébese la Sección Segunda del Reglamento de Organización y Funciones del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), aprobado por Decreto Supremo N° 104-2021-PCM, que consta de un (1) título, treinta y seis (36) artículos; así como la Estructura Orgánica y el Organigrama del INDECOPI, que como anexos forman parte integrante de la presente Resolución.

39

DECRETO SUPREMO 032-2021-PCM, DECRETO SUPREMO QUE APRUEBA LA GRADUACIÓN, METODOLOGÍA Y FACTORES PARA LA DETERMINACIÓN DE LAS MULTAS QUE IMPONGAN LOS ÓRGANOS RESOLUTIVOS DEL INDECOPI RESPECTO DE LAS INFRACCIONES SANCIONABLES EN EL ÁMBITO DE SU COMPETENCIA, publicado en el Diario Oficial El Peruano el 25 de febrero de 2021.

Artículo 1. Objeto

El presente Decreto Supremo tiene por objeto aprobar la graduación, metodología y factores para la determinación de las multas que impongan los órganos resolutivos del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI respecto de las infracciones sancionables en el ámbito de su competencia que, como Anexo forma parte integrante del presente Decreto Supremo.
(Subrayado agregado)

40

LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de setiembre de 2010 y modificado por Decreto Legislativo N° 1308, publicado en el Diario Oficial El Peruano el 30 de diciembre de 2016.

Artículo 107.- Postulación del procedimiento.

Los procedimientos administrativos para conocer las presuntas infracciones a las disposiciones contenidas en el presente Código se inician de oficio, bien por propia iniciativa de la autoridad, por denuncia del consumidor afectado o del que potencialmente pudiera verse afectado, o por una asociación de consumidores en representación de sus asociados o poderdantes o en defensa de intereses colectivos o difusos de los consumidores. En este último caso, la asociación de consumidores actúa como tercero legitimado sin gozar de las facultades para disponer derechos de los consumidores

108. En esa línea, el Decreto Supremo N° 032-2021-PCM, estableció tres (3) métodos para para la graduación de las sanciones, denominados: (i) *método basado en valores preestablecidos*; (ii) *método basado en un porcentaje de las ventas del producto o servicio afectado*; y, (iii) *método ad hoc*. Asimismo, respecto del *método basado en valores preestablecidos* se precisó que este se subdividía para cuatro (4) supuestos:
- (i) Método de valores preestablecidos para infracciones vinculadas con el Libro de Reclamaciones.
 - (ii) Método de valores preestablecidos para las infracciones a las normas de eliminación de barreras burocráticas.
 - (iii) Método de valores preestablecidos para infracciones de Prestadores de Servicios de Certificación Digital.
 - (iv) Método de valores preestablecidos para otras infracciones en OPS, CPC y SPC.
109. Así, de acuerdo a lo señalado en el Decreto Supremo N° 032-2021-PCM, el órgano resolutor de segunda instancia, al conocer determinado procedimiento en vía de apelación, debe aplicar el mismo método de graduación que le corresponde al órgano resolutor de primera instancia; en ese sentido, el *método de valores preestablecidos para infracciones vinculadas con el Libro de Reclamaciones* y el *método de valores preestablecidos para otras infracciones en OPS CPC y SPC* serán los aplicables para este órgano colegiado cuando actúe como superior jerárquico⁴¹.

afectados, salvo de sus asociados o de las personas que le hayan otorgado poder para tal efecto. Tanto el consumidor constituido como parte como el tercero legitimado pueden participar en el procedimiento e interponer los recursos contra la resolución que deniegue el inicio del procedimiento y contra cualquier otra resolución impugnada que les produzca agravio. El procedimiento administrativo en materia de protección al consumidor se inicia con la notificación de la imputación de cargos al posible infractor

41

DECRETO SUPREMO 032-2021-PCM, DECRETO SUPREMO QUE APRUEBA LA GRADUACIÓN, METODOLOGÍA Y FACTORES PARA LA DETERMINACIÓN DE LAS MULTAS QUE IMPONGAN LOS ÓRGANOS RESOLUTIVOS DEL INDECOPI RESPECTO DE LAS INFRACCIONES SANCIONABLES EN EL ÁMBITO DE SU COMPETENCIA, publicado en el Diario Oficial El Peruano el 25 de febrero de 2021.

ANEXO

GRADUACIÓN, METODOLOGÍA Y FACTORES PARA LA DETERMINACIÓN DE LAS MULTAS QUE IMPONGAN LOS ÓRGANOS RESOLUTIVOS DEL INDECOPI RESPECTO DE LAS INFRACCIONES SANCIONABLES EN EL ÁMBITO DE SU COMPETENCIA

Capítulo I: Pasos para la estimación de multas

(....)

En ese sentido, el proceso de estimación de multas en el Indecopi cuenta con tres grandes etapas, las cuales se mencionan de forma general a continuación:2

A. Estimación de la Multa Base (m)

El monto de la Multa Base (m) comprende una aproximación directa o indirecta del beneficio ilícito o afectación (perjuicio económico o daño) generada por el infractor (dentro de un espacio y tiempo determinado) y del grado de disuasión deseado.

La metodología para la determinación de la Multa Base (m) de los OR del INDECOPI considera los siguientes tres tipos de aproximaciones:

- i. Método basado en valores preestablecidos;
- ii. Método basado en un porcentaje de las ventas del producto o servicio afectado;
- iii. Método ad hoc.

El detalle metodológico de cada aproximación es desarrollado en el Capítulo II del presente Anexo.

El Cuadro 1 muestra el detalle de las aproximaciones a utilizar según cada OR.

Cuadro N° 1

APROXIMACIONES METODOLÓGICAS PARA EL CÁLCULO DE MULTAS POR MATERIA Y ÓRGANO RESOLUTIVO

Materia	Método
---------	--------

110. El método basado en valores preestablecidos para otras infracciones en OPS CPC y SPC será utilizado para aquellas infracciones al Código que sean distintas a las infracciones vinculadas al Libro de Reclamaciones⁴². Así, dicho método establece el esquema y los factores que se deben tener presente, es decir, la Multa Preliminar (M) será el resultado de multiplicar el valor estimado de la Multa Base (m) por un componente que captura el efecto de las circunstancias agravantes y atenuantes presente en cada caso (F). Finalmente, dicho monto (M) es ajustado conforme a los topes máximos legales pertinentes, hasta obtener una Multa Final (M*)⁴³, tal como se aprecia a continuación:

Diagrama N° 1

	Órgano Resolutivo ^{1/}	Preestablecido	Porcentaje de las ventas del producto o servicio afectado	Ad hoc
Protección del Consumidor	OPS / CPC	P / *	-	-
	CPC / SPC	P / *	-	P
Protección de la Propiedad Intelectual ^{2/}	DDA / SPI	*	-	P
	DSD / SPI	*	-	P
	DIN / SPI	*	-	P
Gestión de la Infraestructura Oficial de Firma Electrónica	CFE / SDC	*	-	-
Defensa de la Competencia	CCD / SDC	P	P	-
	CLC / SDC	*	P	P
	CEB / SEL	*	-	-
	CCO / SCO	*	-	P

Nota:

(...)

- 1/ El OR de segunda instancia aplica el mismo método que le corresponde al OR de primera instancia cuando analice las respectivas apelaciones.

(...)

⁴² En este último caso, se deberá utilizar el método de valores preestablecidos para infracciones vinculadas con el Libro de Reclamaciones.

⁴³ **DECRETO SUPREMO 032-2021-PCM, DECRETO SUPREMO QUE APRUEBA LA GRADUACIÓN, METODOLOGÍA Y FACTORES PARA LA DETERMINACIÓN DE LAS MULTAS QUE IMPONGAN LOS ÓRGANOS RESOLUTIVOS DEL INDECOPI RESPECTO DE LAS INFRACCIONES SANCIONABLES EN EL ÁMBITO DE SU COMPETENCIA, publicado en el Diario Oficial El Peruano el 25 de febrero de 2021.**

ANEXO

GRADUACIÓN, METODOLOGÍA Y FACTORES PARA LA DETERMINACIÓN DE LAS MULTAS QUE IMPONGAN LOS ÓRGANOS RESOLUTIVOS DEL INDECOPI RESPECTO DE LAS INFRACCIONES SANCIONABLES EN EL ÁMBITO DE SU COMPETENCIA

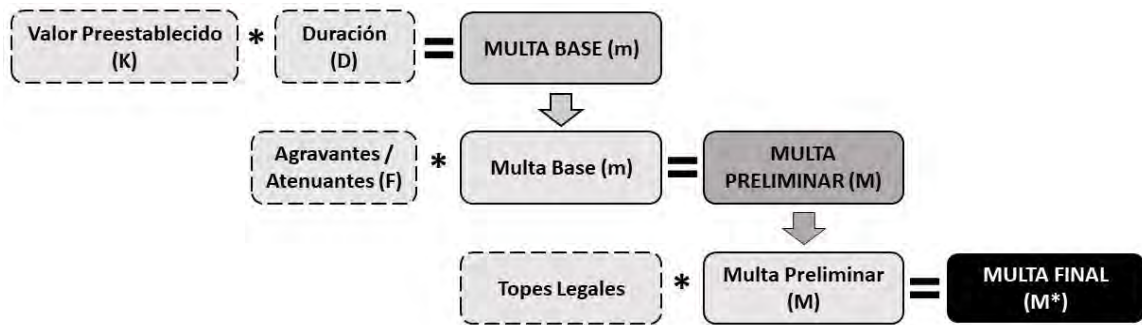
Capítulo I: Pasos para la estimación de multas

Sobre la base de la revisión del proceso de graduación de sanciones por parte de los OR del Indecopi, se tiene que, en términos generales, la multa preliminar (M) es el resultado de multiplicar el valor estimado de la multa base (m) por un componente que captura el efecto de las circunstancias agravantes y atenuantes presentes en cada caso (F), conforme a la siguiente fórmula:

$$(I) M = m \times F$$

Finalmente, dicho monto (M) es ajustado conforme a los topes máximos legales pertinentes, hasta obtener una multa final (M*).

(....).



—Multa Base (m)

111. De acuerdo con el diagrama planteado, la Multa Base (m) se estima multiplicando un primer componente de valor preestablecido (K) por un segundo componente de factor de duración (D)⁴⁴. Para la determinación de cada uno de los elementos mencionados, debemos considerar lo siguiente:

a) **Determinación del valor preestablecido (K)**

112. El valor preestablecido (K) se determina a partir de un cuadro de doble entrada ordenada, por filas, según el nivel de afectación (subíndice K_i) y, en columnas, según el tamaño del infractor (subíndice K_j), conforme al Cuadro 18 del Decreto Supremo N° 032-2021-PCM:

**“Cuadro N° 18
OPS - PERÚ y CPC - PERÚ (CUANDO ACTÚE COMO SEGUNDA INSTANCIA): MONTO
PREESTABLECIDO DE $k_{i,j}$, POR TAMAÑO DEL INFRACTOR, SEGÚN TIPO DE AFECTACIÓN (UIT)**

Nivel de afectación (K_i)	Tamaño del infractor (K_j)			
	Microempresa o persona natural	Pequeña empresa	Mediana empresa	Gran empresa
Muy baja	1,01	1,09	2,02	3,00
Baja	1,55	1,93	2,57	3,49
Moderada	2,02	2,42	3,00	3,78
Alta	3,01	3,07	3,95	4,01
Muy alta	5,13	5,46	5,47	5,48”

113. El nivel de afectación (subíndice K_i) se establece según el tipo de infracción asociada a cada caso en particular y se utiliza para los procedimientos administrativos de apelación (segunda instancia), la clasificación contenida en el Cuadro 16 del Decreto Supremo

⁴⁴ DECRETO SUPREMO 032-2021-PCM, DECRETO SUPREMO QUE APRUEBA LA GRADUACIÓN, METODOLOGÍA Y FACTORES PARA LA DETERMINACIÓN DE LAS MULTAS QUE IMPONGAN LOS ÓRGANOS RESOLUTIVOS DEL INDECOPI RESPECTO DE LAS INFRACCIONES SANCIONABLES EN EL ÁMBITO DE SU COMPETENCIA, publicado en el Diario Oficial El Peruano el 25 de febrero de 2021.
(...)

A.4 Método de valores preestablecidos para otras infracciones en OPS, CPC y SPC, así como en los casos de CCD, SDC, DSD, DDA, DIN y SPI

Bajo la aproximación de valores preestablecidos para otras infracciones en OPS, CPC y SPC, así como en los casos de CCD, SDC, DSD, DDA, DIN10 y SPI, la Multa Base (m) se estima multiplicando un primer componente de valores preestablecidos según la afectación y el tamaño del infractor ($k_{i,j}$) por un segundo componente que denominamos factor de Duración (Dt), conforme la siguiente expresión:

(VI) $m = k_{i,j} \times Dt$

N° 032-2021-PCM⁴⁵, cuyo resultado evidenciará si nos encontramos ante una infracción muy alta, *alta, moderada, baja* o *muy baja*.

45

DECRETO SUPREMO 032-2021-PCM, DECRETO SUPREMO QUE APRUEBA LA GRADUACIÓN, METODOLOGÍA Y FACTORES PARA LA DETERMINACIÓN DE LAS MULTAS QUE IMPONGAN LOS ÓRGANOS RESOLUTIVOS DEL INDECOPI RESPECTO DE LAS INFRACCIONES SANCIONABLES EN EL ÁMBITO DE SU COMPETENCIA, publicado en el Diario Oficial El Peruano el 25 de febrero de 2021.

(...)

a) Determinación de *ki,j*

El primer componente (*ki,j*) se determina a partir de un cuadro de doble entrada ordenada por filas conforme el nivel de afectación (subíndice *i*) y en columnas según el tamaño de infractor (subíndice *j*).¹²

En el caso de los OPS, CPC y SPC, los niveles de afectación son determinados de acuerdo con el tipo de infracción asociada a cada caso en particular, considerando el detalle del Cuadro 16.

Cuadro N° 16
OPS, CPC y SPC- PERÚ: TIPO DE AFECTACIÓN, SEGÚN TIPO DE INFRACCIÓN

Niveles de Afectación	Tipo de Infracción
Muy Alta	-Infracciones donde se produzca una afectación al trato diferenciado o discriminación, dignidad y/o reputación y normas de convivencia.
Alta	- Infracciones donde la cuantía afectada del bien o servicio denunciado sea superior a (02) UIT si son analizadas por los OPS, y superior a (08) UIT si son analizadas por la CPC a excepción de CC3 que analiza casos de oficio que pueden alcanzar otra escala de la cuantía ^{1/2/} . - Infracciones que afectan un interés colectivo o difuso (que no estén asociadas a los demás tipos de infracción precisados en esta tabla), cuya cuantía afectada total de los bienes o servicios considerados en el procedimiento sea mayor a (104) UIT ^{3/} . - Infracciones que puedan generar afectaciones a la subsistencia del consumidor. - Infracciones relativas a métodos comerciales coercitivos, métodos comerciales agresivos o engañosos, y métodos abusivos de cobranza que afecten la integridad del consumidor (agravios). - Infracciones sobre modificaciones contractuales o cláusulas abusivas que afecten la integridad del consumidor.
Moderada	- Infracciones donde la cuantía afectada del bien o servicio denunciado sea superior a (01) UIT y menor a (02) UIT si son analizadas por los OPS, y superior a (04) UIT y menor a (08) UIT si son analizadas por la CPC (a excepción de CC3 que analiza casos de oficio que pueden alcanzar otra escala de la cuantía). - Infracciones que afectan un interés colectivo o difuso (que no estén asociadas a los demás tipos de infracción precisados en esta tabla), cuya cuantía afectada total de los bienes o servicios considerados en el procedimiento sea mayor a (30) UIT y menor a (104) UIT ^{3/} . - Infracciones sobre modificaciones contractuales o cláusulas abusivas que impliquen una afectación económica del consumidor. - Infracciones relativas a métodos comerciales coercitivos, métodos comerciales agresivos o engañosos, y métodos abusivos de cobranza que tengan afectaciones materiales o económicas.
Baja	- Infracciones donde la cuantía afectada del bien o servicio denunciado sea menor a (01) UIT si son analizadas por los OPS, y superior a (03) UIT y menor a (04) UIT si son analizadas por las CPC (a excepción de CC3 que analiza casos de oficio que pueden alcanzar otra escala de la cuantía). - Infracciones que afectan un interés colectivo o difuso (que no estén asociadas a los demás tipos de infracción precisados en esta tabla), cuya cuantía afectada total de los bienes o servicios considerados en el procedimiento sea menor a (30) UIT. ^{3/} - Infracciones asociadas a atención de reclamos, atención de requerimientos de información del consumidor que involucren una falsedad, solicitudes de gestión y requerimientos de información de la Autoridad (cuando afectan la resolución del caso). - Infracciones sobre modificaciones contractuales o cláusulas abusivas que no impliquen una afectación económica del consumidor o una afectación a la integridad del consumidor. - Infracciones vinculadas a la falta de entrega de contratos y demás documentación relacionada con los actos jurídicos celebrados.
Muy baja	- Infracciones relativas a falta de atención a requerimientos de información del consumidor, y requerimientos de información de la Autoridad (cuando no afectan la resolución del caso). ^{4/} - Incumplimientos de medidas correctivas, medida cautelar, acuerdos conciliatorios y liquidación de costas y costos. ^{5/}

Nota: Cabe destacar que los tipos de infracción señalados en todos los niveles de afectación también aplican para la CC3 (salvo donde se especifique lo contrario).

1/ Por ejemplo, si la infracción es sobre la idoneidad del espejo de un carro, la cuantía afectada se estima en base al valor del espejo y no de todo el carro. De igual manera si la infracción corresponde al no envío de un estado de cuenta,

114. El tamaño del infractor (subíndice Kj) se establece considerando la clasificación de las empresas conforme a su nivel de ventas en UIT, atendiendo a lo establecido en el Texto Único Ordenado de la Ley de Impulso al Desarrollo Productivo y al Crecimiento Empresarial, aprobado por Decreto Supremo N° 013-2013-PRODUCE (en adelante, Ley Mype)⁴⁶, según el cuadro siguiente:

Cuadro N° 1

Tipo de empresa	Valor de venta
Microempresa	Desde 1 UIT hasta 150 UIT
Pequeña empresa	Superior a 150 UIT hasta 1 700 UIT
Mediana Empresa	Superior a 1700 UIT hasta 2 300 UIT
Gran empresa	Superior a 2 300 UIT

*Cuadro elaborado por la Secretaría Técnica sobre la base de lo indicado en el Decreto Supremo N° 032-2021-PCM.

115. Ahora bien, este Colegiado advierte que el *método basado en valores preestablecidos para otras infracciones en OPS, CPC y SPC* no ha contemplado qué ejercicio (año) se tomará en cuenta para valorar las ventas o ingresos del proveedor y qué criterio deberá considerarse en caso de que la autoridad no pueda obtener la información, aspectos relevantes para la determinación del tamaño del infractor.
116. Así, la Comisión advierte que el *método basado en valores preestablecidos para infracciones del Libro de Reclamaciones* establece que se tomará en cuenta el volumen de ventas percibidos por la empresa infractora el año en que cometió la infracción (en caso se tratase de un ejercicio concluido) o, en su defecto, el del inmediato anterior.

la cuantía afectada se valoraría en base al servicio de envío de este estado de cuenta específicamente y no sobre el valor de la cuenta.

2/ Respecto a las infracciones que dependen de la cuantía del bien o servicio específico, los umbrales han sido determinados conforme el siguiente detalle:

- Para los OPS, como los terciles del rango establecido hasta el valor máximo de 3 UIT dispuesto en la Ley N° 29571.
- Para las CPC (excepto CC3, porque no le aplica), como los valores promedios de los montos preestablecidos en los tipos de afectación baja y moderada.

3/ Los umbrales de la cuantía afectada en las infracciones de interés colectivo o difuso fueron determinados a partir de los terciles del valor estimado de la cuantía afectada de los bienes y servicios de una muestra de casos de intereses colectivos o difusos.

4/ Infracciones establecidas en el artículo 5 del Decreto Legislativo N° 807.

5/ Aplicable en tanto se cumpla con lo dispuesto en los artículos 117 y 118 del Código de Protección y Defensa del Consumidor.

46

TEXTO ÚNICO ORDENADO DE LA LEY DE IMPULSO AL DESARROLLO PRODUCTIVO Y AL CRECIMIENTO EMPRESARIAL, aprobado por **DECRETO SUPREMO 013-2013-PRODUCE**, publicado el 28 de diciembre de 2013, y modificada por la **LEY N° 30056, LEY QUE MODIFICA DIVERSAS LEYES PARA FACILITAR LA INVERSIÓN, IMPULSAR EL DESARROLLO PRODUCTIVO Y EL CRECIMIENTO EMPRESARIAL**

Artículo 5.- Características de las micro, pequeñas y medianas empresas

Las micro, pequeñas y medianas empresas deben ubicarse en alguna de las siguientes categorías empresariales, establecidas en función de sus niveles de ventas anuales:

Microempresa: ventas anuales hasta el monto máximo de 150 Unidades Impositivas Tributarias (UIT).

Pequeña empresa: ventas anuales superiores a 150 UIT y hasta el monto máximo de 1700 Unidades Impositivas Tributarias(UIT).

Mediana empresa: ventas anuales superiores a 1700 UIT y hasta el monto máximo de 2300 UIT. El incremento en el monto máximo de ventas anuales señalado para la micro, pequeña y mediana empresa podrá ser determinado por decreto supremo refrendado por el Ministro de Economía y Finanzas y el Ministro de la Producción cada dos (2) años.

Las entidades públicas y privadas promoverán la uniformidad de los criterios de medición a fin de construir una base de datos homogénea que permita dar coherencia al diseño y aplicación de las políticas públicas de promoción y formalización del sector.

Asimismo, en caso no se pueda obtener la información, podrá realizarse una estimación de dichas ventas o ingresos en base a la mejor información disponible⁴⁷.

117. En ese sentido, en virtud de los principios de legalidad y uniformidad de la actuación administrativa⁴⁸, la Comisión tomará en cuenta lo indicado en el párrafo precedente para determinar el ejercicio (año) de los ingresos o ventas del proveedor denunciado y el criterio a utilizarse en caso no se pueda obtener información del proveedor denunciado, ambos aspectos para establecer el tamaño del infractor.

b) Determinación del factor de Duración (D)

118. El factor de Duración (D) se encuentra asociado al tiempo de duración de la infracción, siendo necesario para ello determinar si nos encontramos ante una infracción de

⁴⁷ **DECRETO SUPREMO 032-2021-PCM, DECRETO SUPREMO QUE APRUEBA LA GRADUACIÓN, METODOLOGÍA Y FACTORES PARA LA DETERMINACIÓN DE LAS MULTAS QUE IMPONGAN LOS ÓRGANOS RESOLUTIVOS DEL INDECOPI RESPECTO DE LAS INFRACCIONES SANCIONABLES EN EL ÁMBITO DE SU COMPETENCIA, publicado en el Diario Oficial El Peruano el 25 de febrero de 2021.**

(...)

1/ Los rangos de facturación deben considerarse en función de las ventas o ingresos percibidos por el infractor del año en el que se cometió la infracción (en caso de tratarse de un ejercicio concluido), o en su defecto, el del inmediato anterior. De no contar con la mencionada información, puede realizarse una estimación de dichas ventas o ingresos en base a la mejor información disponible.

- Factor (FC_i):

$$(III) \quad FC_i = \frac{1-FC_0}{1-A_0} (A_i - A_0) + FC_0$$

Dónde:

FC_i: Es el factor corregido por rango de multa que relaciona la facturación de la empresa específica con un valor de multa en el rango establecido.

A_i: Es el valor de la facturación anual de la empresa sujeta a sanción entre el tamaño de la empresa más grande del rango de facturación.

$$(IV) \quad A_i = \frac{\text{Facturación de la empresa infractora}}{\text{Facturación máxima según tipo de empresa}}$$

Para la Mediana y Gran Empresa, se considera una facturación máxima de 20,000 UIT.

FC₀: Cociente de la multa más baja y la multa más alta del respectivo rango.

A₀: Cociente entre la facturación de la empresa más pequeña dentro de su rango y la facturación de la empresa más grande de su respectivo rango.

⁴⁸ **DECRETO SUPREMO N° 004-2019-JUS, TEXTO ÚNICO ORDENADO DE LA LEY N° 27444, LEY DEL PROCEDIMIENTO ADMINISTRATIVO GENERAL, publicado el 25 de enero de 2019**

Artículo IV. Principios del procedimiento administrativo

1. El procedimiento administrativo se sustenta fundamentalmente en los siguientes principios, sin perjuicio de la vigencia de otros principios generales del Derecho Administrativo:

1.1. Principio de legalidad.- Las autoridades administrativas deben actuar con respeto a la Constitución, la ley y al derecho, dentro de las facultades que le estén atribuidas y de acuerdo con los fines para los que les fueron conferidas.

(...)

1.14. Principio de uniformidad.- La autoridad administrativa deberá establecer requisitos similares para trámites similares, garantizando que las excepciones a los principios generales no serán convertidos en la regla general. Toda diferenciación deberá basarse en criterios objetivos debidamente sustentados.

(...)

2. Los principios señalados servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de las reglas de procedimiento, como parámetros para la generación de otras disposiciones administrativas de carácter general, y para suplir los vacíos en el ordenamiento administrativo.

naturaleza instantánea⁴⁹, continuada o permanente⁵⁰. Luego de ello, el tiempo será medido en meses hasta el tope de dos (2) años (o 24 meses); así, según el Decreto Supremo N° 032-2021-PCM, los valores de dicho factor se han determinado de acuerdo con el cuadro siguiente:

**“Cuadro N° 23
FACTOR DE GRADUACIÓN POR EL PERÍODO DE DURACIÓN DEL HECHO INFRACITOR, SEGÚN
MESES**

Duración de la infracción	Factor de Duración (D)
<i>Si la infracción duró hasta 4 meses</i>	1,0
<i>Si la infracción duró entre 5 y 8 meses</i>	1,2
<i>Si la infracción duró entre 9 y 12 meses</i>	1,4
<i>Si la infracción duró entre 13 y 16 meses</i>	1,6
<i>Si la infracción duró entre 17 y 20 meses</i>	1,8
<i>Si la infracción duró entre 21 y 24 meses</i>	2,0”

—Multa Preliminar (M)

119. La Multa Preliminar (M) se obtendrá de la multiplicación de Multa Base (m) por la valoración de atenuantes y agravantes (F); siendo que, para la determinación de este último factor, se considerará lo siguiente:

a) Determinación de (F)

120. Para determinar la valoración de atenuantes y agravantes (F), se deberá analizar y definir si existen circunstancias agravantes y/o atenuantes que corresponda aplicarse. En caso de no existir ninguna circunstancia agravante o atenuante, dicho factor será equivalente a 1 o 100%. De verificarse circunstancias atenuantes o agravantes se establecerá el porcentaje en que cada atenuante y/o agravante disminuye o aumenta, respectivamente, el valor de la Multa Base (m), según lo determinado en el Cuadro N° 2

⁴⁹ **DECRETO SUPREMO 032-2021-PCM, DECRETO SUPREMO QUE APRUEBA LA GRADUACIÓN, METODOLOGÍA Y FACTORES PARA LA DETERMINACIÓN DE LAS MULTAS QUE IMPONGAN LOS ÓRGANOS RESOLUTIVOS DEL INDECOPI RESPECTO DE LAS INFRACCIONES SANCIONABLES EN EL ÁMBITO DE SU COMPETENCIA, publicado en el Diario Oficial El Peruano el 25 de febrero de 2021.**

(...)

El hecho infractor puede ser instantáneo (empieza y termina con el mismo acto), continuado (la infracción dura por un periodo de tiempo) o permanente (la infracción permanece en el tiempo). Asimismo, el hecho infractor puede durar desde el inicio del acto hasta el cese de éste o como máximo hasta la fecha de notificación de la imputación de cargos; sin embargo, no deberá considerarse como parte de la duración de la infracción el tiempo que tardó el demandante en presentar su denuncia desde la fecha en que se ejecutó la infracción, a menos que dicho periodo de tiempo esté asociado a la duración real de la infracción.

⁵⁰ *“Es instantánea cuando “la lesión o puesta en peligro del bien jurídico protegido se produce en un momento determinado, en el que la infracción se consume, sin producir una situación antijurídica duradera”, es infracción instantánea con efectos permanentes, cuando se genera “un estado de cosas contrario a/ ordenamiento jurídico, que se mantiene. (...) aunque los efectos de la conducta infractora sean duraderos y permanezcan en el tiempo, la consumación de esta es instantánea, por lo que es a partir de este momento en que debe contarse el plazo de prescripción de la infracción”; es infracción continuada, cuando “se realizan diferentes conductas, cada una de las cuales constituye por separado una infracción, pero que se consideran como una única infracción, siempre y cuando formen parte de un proceso unitario y, finalmente, es infracción permanente aquella en donde el administrado se mantiene en una situación infractora, cuyo mantenimiento le es imputable (...) no son los efectos jurídicos de la conducta infractora los que persisten, sino la conducta misma”.* BACA ONETO, Víctor Sebastián. La prescripción de las infracciones y su clasificación en la Ley del Procedimiento Administrativo General. Revista Derecho & Sociedad N° 37. Año 2012. P.268.

del Decreto Supremo N° 032-2021-PCM⁵¹. Para mejor ilustración, a manera de ejemplo, se muestra lo siguiente:

Cuadro N° 2

Ejemplos de circunstancias agravantes
Reincidencia (cuando el administrado ha sido sancionado mediante resolución firme por una infracción igual a la que se le imputa, dentro del plazo de un año como máximo). ⁵²
Reiterancia (cuando el administrado continúa incurriendo en la conducta infractora pese a la advertencia de la autoridad). ⁵³

⁵¹ **DECRETO SUPREMO 032-2021-PCM, DECRETO SUPREMO QUE APRUEBA LA GRADUACIÓN, METODOLOGÍA Y FACTORES PARA LA DETERMINACIÓN DE LAS MULTAS QUE IMPONGAN LOS ÓRGANOS RESOLUTIVOS DEL INDECOPI RESPECTO DE LAS INFRACCIONES SANCIONABLES EN EL ÁMBITO DE SU COMPETENCIA, publicado en el Diario Oficial El Peruano el 25 de febrero de 2021.**

B. Valoración de atenuantes y agravantes (F)

Este segundo paso corresponde a la valoración de las circunstancias que pueden incrementar (agrarar) o reducir (atenuar) el monto de la multa base, a través del factor F. Para determinar el valor del factor F, los OR deben realizar el siguiente análisis:

- Definir si existen circunstancias agravantes o atenuantes que correspondan aplicar.
- En caso de no existir ninguna circunstancia agravante y atenuante, el factor F es equivalente a la unidad (F = 1 o 100 %).
- En caso de verificar circunstancias agravantes o atenuantes (f_i), se debe establecer el porcentaje en que cada atenuante y/o agravante disminuye y/o aumenta, respectivamente, el valor de m. Para esto, se debe sumar todos los porcentajes (f_i), y se le agrega la unidad (o 100%). Esto puede realizarse mediante la siguiente expresión:

$$(II) \quad F = 1 + (f_1 + f_2 + f_3 \dots f_n) = 1 + \sum_{i=1}^n f_i$$

Donde n representa al número de circunstancias agravantes y atenuantes identificadas.

Cabe mencionar que las circunstancias atenuantes pueden reducir la multa base hasta en un 50% y que las circunstancias agravantes pueden incrementarla hasta en un 100%.

En caso el OR determine que el hecho infractor presenta algunas de las circunstancias agravantes o atenuantes que figuran en el Cuadro 2, debe considerar los valores señalados en dicho cuadro, en tanto sean compatibles con su marco legal especial. Por ende, pueden existir casos en los que el marco normativo establece circunstancias atenuantes o agravantes específicas y sus respectivos valores de reducción o incremento, en cuyo caso prima lo indicado en dicho marco normativo en consideración de su respectiva jerarquía, pero tratando de conciliar en lo posible dicho criterio con el presente Decreto Supremo.

Cabe señalar que los OR pueden considerar otras circunstancias atenuantes o agravantes adicionales a las que se presentan en el Cuadro 2, siempre que sean pertinentes de acuerdo con las características de cada caso en particular y en la medida que su marco legal especial se lo permita.

⁵² **TEXTO ÚNICO ORDENADO DE LA LEY DEL PROCEDIMIENTO ADMINISTRATIVO GENERAL, aprobado por DECRETO SUPREMO N° 004-2019-JUS y publicado el 25 de enero de 2019**

Artículo 248.- Principios de la potestad sancionadora administrativa

La potestad sancionadora de todas las entidades está regida adicionalmente por los siguientes principios especiales:

(...)

3. Razonabilidad.- Las autoridades deben prever que la comisión de la conducta sancionable no resulte más ventajosa para el infractor que cumplir las normas infringidas o asumir la sanción. Sin embargo, las sanciones a ser aplicadas deben ser proporcionales al incumplimiento calificado como infracción, observando los siguientes criterios que se señalan a efectos de su graduación:

(...)

e) La reincidencia, por la comisión de la misma infracción dentro del plazo de un (1) año desde que quedó firme la resolución que sancionó la primera infracción.

(...).

⁵³ "(...) la autoridad administrativa deberá considerar la reincidencia (cuando el administrado ya ha sido sancionado por una infracción análoga o igual a la que se le imputa) o reiterancia (cuando el administrado continúa incurriendo en la conducta infractora pese a la advertencia de la autoridad), como un factor que determina el incremento de las sanciones (...).

GOMEZ APAC, Hugo y VERGARAY BÉJAR, Verónica. (2009). La potestad sancionadora y los principios del procedimiento sancionador. Lima: Fondo Editorial de la Universidad de Ciencias Aplicadas. Recuperado de https://www.mpfm.gob.pe/escuela/contenido/actividades/docs/2275_potestad_sancionadora_veronica_vergaray_hugo_gomez.pdf

La conducta del denunciado a lo largo del procedimiento que contravenga el principio de conducta procedimental.
Cuando la conducta infractora haya puesto en riesgo u ocasionado daño a la salud, la vida o la seguridad de personas. ⁵⁴
Cuando el denunciado, teniendo conocimiento de la conducta infractora, deja de adoptar las medidas necesarias para evitar o mitigar sus consecuencias.
Cuando la conducta infractora haya afectado el interés colectivo o difuso.
Ejemplos de circunstancias atenuantes
La presentación por el denunciado de una propuesta conciliatoria dentro del procedimiento administrativo que coincida con la medida correctiva ordenada por el órgano resolutorio.
Cuando el denunciado acredite haber concluido con la conducta ilegal tan pronto tuvo conocimiento de esta y haber iniciado las acciones necesarias para remediar los efectos adversos de la misma.
Cuando el denunciado reconoce las imputaciones o se allana a las pretensiones después de la presentación de sus descargos.
Cuando el administrado reconoce su responsabilidad de forma expresa y por escrito con anterioridad y posterioridad al Informe Final de Instrucción.
Cuando el denunciado acredite que cuenta con un programa efectivo para el cumplimiento de la regulación contenida en la normativa.

*Cuadro elaborado por la Secretaría Técnica sobre la base de lo indicado en el Decreto Supremo N° 032-2021-PCM.

—Multa Final (M*)

121. Finalmente, para determinar la Multa Final (M*) se deberá obtener de la comparación entre la Multa Preliminar (M) y el tope máximo establecido por la normativa vigente⁵⁵. Así, en dicha comparación se verificará que la Multa Preliminar (M) no supere el tope establecido en el marco normativo para los procedimientos de protección al consumidor,

⁵⁴ **DECRETO SUPREMO 032-2021-PCM, DECRETO SUPREMO QUE APRUEBA LA GRADUACIÓN, METODOLOGÍA Y FACTORES PARA LA DETERMINACIÓN DE LAS MULTAS QUE IMPONGAN LOS ÓRGANOS RESOLUTIVOS DEL INDECOPI RESPECTO DE LAS INFRACCIONES SANCIONABLES EN EL ÁMBITO DE SU COMPETENCIA, publicado en el Diario Oficial El Peruano el 25 de febrero de 2021.**

B. Valoración de atenuantes y agravantes (F)

1/ Siempre y cuando, a efectos de evitar duplicidad, la multa base no incorpore el valor del riesgo o daño a la vida estimado mediante el enfoque ad-hoc. Por otro lado, entiéndase el riesgo como aquella situación en la que existe la posibilidad de ocurrencia de un evento incierto y que a la vez también lleve a un determinado resultado.

⁵⁵ **DECRETO SUPREMO 032-2021-PCM, DECRETO SUPREMO QUE APRUEBA LA GRADUACIÓN, METODOLOGÍA Y FACTORES PARA LA DETERMINACIÓN DE LAS MULTAS QUE IMPONGAN LOS ÓRGANOS RESOLUTIVOS DEL INDECOPI RESPECTO DE LAS INFRACCIONES SANCIONABLES EN EL ÁMBITO DE SU COMPETENCIA, publicado en el Diario Oficial El Peruano el 25 de febrero de 2021.**

(...)

C. Ajuste de la multa según topes legales (determinación de la multa final M*)

En este paso se analiza si la multa preliminar (M) se encuentra dentro del tope máximo establecido en el marco normativo de cada OR, el cual puede estar expresado en función del monto máximo a imponer en términos de Unidades Impositivas Tributarias (N°UIT) o en términos de un porcentaje máximo de los ingresos totales de la empresa infractora en el último año (%IT).

Así, el OR verifica que la multa preliminar (M) no supere el tope establecido en su marco normativo; en caso contrario, debe limitar el monto de la multa final al valor del tope establecido en su norma. De esa forma, la multa final a imponer (M*) queda determinada conforme a la siguiente expresión:

$$(I) \quad M^* \cong \text{Mín}\{M, N^{\circ}UIT, \%IT\}$$

Donde Mín representa el valor mínimo de los elementos en consideración.

Es preciso señalar que los OR pueden aplicar medidas no monetarias razonables de mitigación o remediación, conforme a ley (como programas de compromisos, entre otros, que sean de implementación factible y monitoreable) de forma independiente a la multa (siempre que cuenten con habilitación legal para hacerlo). No obstante, también pueden evaluar aplicarlas de manera complementaria con el fin de asegurar los efectos disuasorios pertinentes para el cambio de las conductas y mitigar el riesgo de reincidencia.

según el artículo 110 del Código⁵⁶; caso contrario, debe limitarse el monto de la multa final al valor del tope establecido en la normativa.

—Aplicación al caso en concreto

122. En el presente caso, el procedimiento administrativo formulado contra el Banco, por presunta infracción al Código, inició el 13 de setiembre de 2023, fecha en que se notificó con la imputación de cargos al proveedor denunciado; por lo que, corresponde aplicar la nueva graduación, metodología y factores para la determinación de las multas establecido por el Decreto Supremo N° 032-2021-PCM.
123. Dicho esto, se verifica que la Comisión ha revocado el pronunciamiento de OPS, declarando fundada la presente denuncia contra el Banco por lo que, corresponde realizar una graduación de la sanción respectiva.
124. Asimismo, para la aplicación del *método de valores preestablecidos para otras infracciones en OPS, CPC y SPC*, se advierte que la infracción incurrida cumple con lo siguiente: (i) se desarrolló por un periodo menor a dos (2) años; (ii) no dañó ni puso en riesgo la vida y/o salud de las personas; y, (iii) tuvo un alcance geográfico menor al nivel nacional.
125. Para este caso en particular, a fin de obtener el valor preestablecido (K) se tomó en cuenta que la infracción cometida por el Banco consistió en no haber adoptado las medidas de seguridad pertinentes, al permitir que se debite indebidamente una operación en la Cuenta de Ahorros N° 191-*****0-80 de la denunciante, la cual correspondía a su patrón habitual de consumo. En ese sentido, se verifica, según lo desarrollado en el marco teórico, que la infracción denunciada se encuadra en *“Infracciones donde la cuantía afectada del bien o servicio denunciado sea superior a (01) UIT y menor a (02) UIT.”*
126. Por otro lado, en cuanto al tamaño de la empresa (subíndice Kj) debe indicarse que, de la página web de la Superintendencia de Mercados y Valores (SMV) se verificó que esta

⁵⁶ **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de setiembre de 2010, modificada por el DECRETO LEGISLATIVO 1308, publicado el 30 de diciembre de 2016**

Artículo 110.- Sanciones administrativas

El Indecopi puede sancionar las infracciones administrativas a que se refiere el artículo 108 con amonestación y multas de hasta cuatrocientos cincuenta (450) Unidades Impositivas Tributarias (UIT), las cuales son calificadas de la siguiente manera:

- a. Infracciones leves, con una amonestación o con una multa de hasta cincuenta (50) UIT.
- b. Infracciones graves, con una multa de hasta ciento cincuenta (150) UIT.
- c. Infracciones muy graves, con una multa de hasta cuatrocientos cincuenta (450) UIT.

En el caso de las microempresas, la multa no puede superar el diez por ciento (10%) de las ventas o ingresos brutos percibidos por el infractor, relativos a todas sus actividades económicas, correspondientes al ejercicio inmediato anterior al de la expedición de la resolución de primera instancia, siempre que se haya acreditado dichos ingresos, no se encuentre en una situación de reincidencia y el caso no verse sobre la vida, salud o integridad de los consumidores.

Para el caso de las pequeñas empresas, la multa no puede superar el veinte por ciento (20%) de las ventas o ingresos brutos percibidos por el infractor, conforme a los requisitos señalados anteriormente. La cuantía de las multas por las infracciones previstas en el Decreto Legislativo núm. 807, Ley sobre Facultades, Normas y Organización del Indecopi, se rige por lo establecido en dicha norma, salvo disposición distinta del presente Código.

Las sanciones administrativas son impuestas sin perjuicio de las medidas correctivas que ordene el Indecopi y de la responsabilidad civil o penal que pueda corresponder.

facturó, en el 2022, un importe superior a 2 300 UIT⁵⁷, en aplicación del rango establecido; por lo que, corresponde asignarle el valor de gran empresa. En suma, según lo establecido en el Cuadro N° 1, el valor preestablecido (K) equivale a tres con setenta y ocho (3,78).

127. Ahora bien, en cuanto al factor de duración (D), se evidencia que la infracción tiene naturaleza instantánea, en la medida que la infracción por cargo indebido de una (1) operación no reconocida se configura el mismo día de la realización de esta. Así, este Colegiado estima que su duración fue menor a cuatro (4) meses; por lo que, corresponde aplicar un factor de duración de uno (1). Por ende, considerando los resultados obtenidos del valor preestablecido (K) y el factor de duración (D), la Multa Base (m) de la presente infracción tiene un valor de tres con setenta y ocho (3,78) UIT.
128. De otro lado, en el presente caso, corresponde señalar que la Comisión no evidencia la configuración de algún factor agravante o atenuante (F), lo que implica que dicho factor sea igual a la unidad ($F = 1$ o 100 %). Bajo ese escenario, la Multa Base (m) obtenida no sufre variación y será equivalente a la Multa Preliminar (M). Para una mejor comprensión de los criterios aplicados, graficamos los datos utilizados de la forma siguiente:

Gráfico N° 1

(Ver en la página siguiente)

Revisado el 31 de enero de 2023, en:
https://www.smv.gob.pe/Frm_DetalleInfoFinanciera.aspx?data=00E99F518A79EA30830AF5D359AB895D5848BCCF36D26D9EBC7E076338B69C3AF9969C710B4740FE8F73A1D47734F4E0DB46988430703A0882DDED753DAFD0DEFD1E1878607A8AD8531B0B43251679D5C34170EFA395FAF54A1D70D26F3.

REPORTE DEL CÁLCULO DE MULTAS - PREESTABLECIDO

Órgano resolutivo	CC1
RUC del sancionado	20100047218
Razón social del sancionado	BANCO DE CREDITO DEL PERU
Tamaño del sancionado	Gran empresa
Tipo de infracción	Infracciones donde la cuantía afectada del bien o servicio denunciado sea superior a (01) UIT y menor a (02) UIT.
Nivel de infracción	Moderada
Factor de duración (Dt)	1.00
Multa base (UIT)	3.78
Factores agravantes y atenuantes (F)	1.00
Multa preliminar (UIT)	3.78
No supera los topes legales	
Multa final (UIT) ¹	3.78

129. Finalmente, al verificarse que la Multa Preliminar (M) no supera los topes, así como tomando en consideración los principios de legalidad, predictibilidad y razonabilidad que rigen la actuación de la autoridad administrativa, este Colegiado estima que corresponde imponer al Banco una Multa Final (M*) de tres con setenta y ocho (3,78) UIT.
130. Por lo expuesto, y considerando que la potestad sancionadora otorgada a la autoridad administrativa debe ser ejercida dentro de los parámetros fijados por el ordenamiento y conforme a los principios que inspiran el ejercicio del poder punitivo del Estado; y, adicionalmente, en aplicación del Principio de Razonabilidad que establece el numeral 3 del artículo 248° del TUO de la LPAG⁵⁸, la Comisión considera que corresponde

⁵⁸ **DECRETO SUPREMO N° 006-2017-JUS, TEXTO ÚNICO ORDENADO DE LA LEY 27444, LEY DEL PROCEDIMIENTO ADMINISTRATIVO GENERAL, publicado el 20 de marzo de 2017**

Artículo 246°.- Principios de la potestad sancionadora administrativa

La potestad sancionadora de todas las entidades está regida adicionalmente por los siguientes principios especiales:

(...)

3. Razonabilidad. - Las autoridades deben prever que la comisión de la conducta sancionable no resulte más ventajosa para el infractor que cumplir las normas infringidas o asumir la sanción; así como que la determinación de la sanción considere criterios como la existencia o no de intencionalidad, el perjuicio causado, las circunstancias de la comisión de la infracción y la repetición en la comisión de infracción.

(...)

sancionar al Banco con una multa de tres con setenta y ocho (3,78) UIT, por infracción a los artículos 1 literal c), 18 y 19 de la Ley N° 29571, Código de Protección y Defensa del Consumidor.

Sobre las costas y los costos del procedimiento

131. El artículo 7 del Decreto Legislativo N° 807⁵⁹, dispone que es potestad de la Comisión ordenar el pago de los costos y costas en que hubiera incurrido el interesado o el Indecopi.
132. En el presente caso, en tanto se ha determinado la responsabilidad administrativa del Banco, la Comisión considera que debe ordenársele el pago de las costas del procedimiento a favor de la denunciante.
133. En consecuencia, el Banco deberá cumplir con pagar a la denunciante las costas del procedimiento que, a la fecha, ascienden a la suma de S/ 36,00, en un plazo no mayor a quince (15) días hábiles, contado a partir del día siguiente de notificada la presente resolución⁶⁰.
134. Asimismo, en un plazo no mayor de cinco (5) días hábiles contado a partir del vencimiento del plazo mencionado en el párrafo anterior, el Banco deberá presentar ante el OPS los medios probatorios que acrediten el cumplimiento del mandato ordenado, bajo apercibimiento de imponer una multa coercitiva conforme a lo establecido en el artículo 118 del Código⁶¹.
135. Es pertinente informar que si la denunciante comunica al OPS el incumplimiento del mandato ordenado y el Banco no presentó ante dicho órgano resolutorio los medios probatorios que acrediten que cumplieron con el referido mandato, la autoridad administrativa resolverá con la documentación que obra en el expediente e impondrá la multa coercitiva por incumplimiento de pago de costas liquidadas⁶².

⁵⁹ **LEY SOBRE FACULTADES, NORMAS Y ORGANIZACIÓN DEL INDECOPI, APROBADO POR DECRETO LEGISLATIVO N° 807 y publicada el 18 de abril de 1996**

Artículo 7.- En cualquier procedimiento contencioso seguido ante el Indecopi, la Comisión u Oficina competente, además de imponer la sanción que corresponda, podrá ordenar que el infractor asuma el pago de las costas y costos del proceso en que haya incurrido el denunciante o el Indecopi. En caso de incumplimiento de la orden de pago de costas y costos del proceso, cualquier Comisión u Oficina del Indecopi podrá aplicar las multas previstas en el inciso b) del artículo 38 del Decreto Legislativo N° 716.

⁶⁰ Tasa correspondiente al derecho de presentación de la denuncia.

⁶¹ **LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de setiembre de 2010 y modificada por el DECRETO LEGISLATIVO N° 1308, publicado el 30 de diciembre de 2016**

Artículo 118.- Multas coercitivas por incumplimiento del pago de costas y costos

Si el obligado a cumplir la orden de pago de costas y costos no lo hace, se le impone una multa no menor de una (1) Unidad Impositiva Tributaria (UIT).

En caso de persistir el incumplimiento de lo ordenado, el órgano resolutorio puede imponer una nueva multa, duplicando sucesivamente el monto de la última multa impuesta hasta el límite de cincuenta (50) Unidades Impositivas Tributarias (UIT). La multa que corresponda debe ser pagada dentro del plazo de cinco (5) días hábiles, vencidos los cuales se ordena su cobranza coactiva.

No cabe la impugnación de las multas coercitivas previstas en el presente artículo.

(Subrayado agregado)

⁶² **DIRECTIVA N° 001-2021/DIR-COD-INDECOPI, DIRECTIVA ÚNICA QUE REGULA LOS PROCEDIMIENTOS DE PROTECCIÓN AL CONSUMIDOR PREVISTOS EN EL CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR**

136. Sin perjuicio de ello y, de considerarlo pertinente, una vez que se ponga fin a la instancia administrativa, la denunciante podrá solicitar el reembolso de los montos adicionales en que hubiese incurrido para la tramitación del presente procedimiento; para lo cual deberá presentar una solicitud de liquidación de costas y costos ante el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor N° 1.

Sobre la inscripción del Banco en el Registro de Infracciones y Sanciones del Indecopi

137. El artículo 119° del Código precisa que el Indecopi lleva un registro de las infracciones que se comprueben y de las sanciones que se impongan en los procedimientos por infracción a la normativa de protección al consumidor, con la finalidad de contribuir a la transparencia de las transacciones del mercado⁶³.
138. La referida norma establece que los proveedores que sean sancionados mediante resolución firme en sede administrativa quedan automáticamente registrados en el referido registro por el lapso de cuatro (4) años, contados a partir de la fecha de la resolución.
139. En la medida que a través del presente pronunciamiento se ha verificado la comisión de una infracción al Código por parte del Banco, así como se le ha impuesto una sanción por ello, corresponde ordenar su inscripción en el Registro de Infracciones y Sanciones del Indecopi, una vez que la resolución emitida por este órgano colegiado sea declarada firme en sede administrativa.

RESUELVE

PRIMERO: revocar la Resolución Final N° 1881-2023/PS2 del 26 de octubre de 2023, emitida por el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor N° 2, en el extremo que declaró infundada la denuncia presentada por la señora Cecilia Ximena Arbe Braga contra Banco de Crédito del Perú S.A. y, reformándola, declararla fundada, por infracción a los artículos 1° literal c), 18° y 19° de la Ley N° 29571, Código de Protección y

Ejecución de Mandatos

Artículo 41.- Incumplimiento del pago de costas y costos

41.1 En caso de incumplimiento del mandato de pago de costas y/o costos liquidados, el beneficiario de dicho mandato deberá comunicar este hecho a la autoridad administrativa.

41.2 El órgano resolutivo de procedimientos sumarísimos una vez recibida la comunicación de incumplimiento por parte del beneficiado por el mandato de pago de costas y costos, atendiendo a las circunstancias del caso, podrá otorgar al administrado obligado por el mandato un plazo adicional de dos días (2) hábiles para cumplir con el apercibimiento de comunicar el cumplimiento del mandato impuesto. 41.3 En caso el obligado no acredite el cumplimiento del pago de las costas y costos o se verifique el incumplimiento del mismo, se procede con la imposición de la multa coercitiva, de conformidad a lo dispuesto en el artículo 118 del Código.

41.4 En el caso en el que el obligado apercibido acredite el cumplimiento oportuno del mandato ordenado, el órgano resolutivo deberá comunicar de tal hecho al beneficiado, quien, de considerar que persiste el incumplimiento, podrá solicitar el inicio de un procedimiento administrativo sancionador por incumplimiento de pago de costas y costos previsto en el artículo 106 del Código, debiendo cumplir con realizar el pago del derecho de tramitación, conforme a lo establecido en el Texto Único de Procedimientos Administrativos del INDECOPI.

⁶³ **LEY 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de setiembre de 2010 y modificada por el Decreto Legislativo 1308, publicado el 30 de diciembre de 2016**

Artículo 119.- Registro de infracciones y sanciones

El Indecopi lleva un registro de infracciones y sanciones a las disposiciones del presente Código con la finalidad de contribuir a la transparencia de las transacciones entre proveedores y consumidores y orientar a estos en la toma de sus decisiones de consumo. Los proveedores que sean sancionados mediante resolución firme en sede administrativa quedan automáticamente registrados por el lapso de cuatro (4) años contados a partir de la fecha de dicha resolución. La información del registro es de acceso público y gratuito.



PERÚ

Presidencia
del Consejo de Ministros

INDECOPI

COMISIÓN DE PROTECCIÓN AL CONSUMIDOR N° 1
SEDE CENTRAL

EXPEDIENTE N° 2393-2023/PS2

Defensa del Consumidor, en la medida que se ha verificado que la entidad bancaria no adoptó las medidas de seguridad pertinentes, al permitir que se debite indebidamente una operación en la Cuenta de Ahorros N° 191-*****0-80 de la denunciante, la cual correspondía a su patrón habitual de consumo, de acuerdo con el siguiente detalle:

FECHA	DETALLE	IMPORTE S/
14/07/2023	TRANSF. BCO. SCOTIA B	5 204,80

SEGUNDO: ordenar a Banco de Crédito del Perú S.A., en calidad de medida correctiva, que en un plazo no mayor de quince (15) días hábiles contado a partir del día siguiente de la notificación de la presente resolución, cumpla con restituir en la Cuenta de Ahorros N° 191-*****0-80 el importe de la operación no reconocida declarada fundada en la presente resolución, así como los intereses dejados de percibir por dicho monto, calculados para el periodo comprendido entre a fecha de realización de la operación y la fecha efectiva de extorno, empleando la tasa de rendimiento correspondiente a dicha cuenta; para lo cual, en un plazo no mayor de cinco (5) días hábiles contado a partir del vencimiento del plazo otorgado inicialmente, el proveedor deberá presentar al Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor N° 2 los medios probatorios que acrediten el cumplimiento del mandato ordenado bajo apercibimiento de imponer una multa coercitiva conforme a lo establecido en el artículo 117 de la Ley N° 29571, Código de Protección y Defensa del Consumidor, así como en el numeral 40.3 de la Directiva N° 001-2021/DIR-COD-INDECOPI denominada "Directiva Única que regula los procedimientos de protección al consumidor previstos en el Código de Protección y Defensa del Consumidor".

TERCERO: sancionar a Banco de Crédito del Perú S.A. con una multa de tres con setenta y ocho (3,78) Unidades Impositivas Tributarias, por infracción a los artículos 1° literal c), 18° y 19° a la Ley N° 29571, Código de Protección y Defensa del Consumidor.

CUARTO: requerir a Banco de Crédito del Perú S.A. el cumplimiento espontáneo de la multa impuesta en la presente resolución, bajo apercibimiento de iniciar el medio coercitivo específicamente aplicable, de acuerdo con lo establecido en el numeral 205.4 del artículo 205° del Texto Único Ordenado de la Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS78, precisándose que los actuados serán remitidos a la Unidad de Ejecución Coactiva para los fines de ley.

QUINTO: ordenar a Banco de Crédito del Perú S.A. que, en un plazo no mayor a quince (15) días hábiles contado a partir del día siguiente de la notificación de la presente resolución, cumpla con pagar a la denunciante las costas y costos del presente procedimiento por ser accesorio al pronunciamiento sustantivo; para lo cual en un plazo no mayor de cinco (5) días hábiles contado a partir del vencimiento del plazo otorgado inicialmente, Banco de Crédito del Perú S.A. deberá presentar ante el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor N° 2 los medios probatorios que acrediten el cumplimiento del mandato ordenado, bajo apercibimiento de que se le imponga una multa coercitiva conforme a lo establecido en el artículo 118 de la Ley N° 29571, Código de Protección y Defensa del Consumidor.

SEXTO: disponer la inscripción de Banco de Crédito del Perú S.A en el Registro de Infracciones y Sanciones del Indecopi, una vez que la resolución quede firme en sede

administrativa, conforme a lo establecido en el artículo 119° de la Ley N° 29571, Código de Protección y Defensa del Consumidor.

SÉTIMO: informar a las partes que la presente resolución tiene vigencia desde el día siguiente de su notificación y, de conformidad con lo dispuesto por el artículo 125 de la Ley N° 29571, Código de Protección y Defensa del Consumidor —modificado por el artículo 1 del Decreto Legislativo N° 1308—, agota la vía administrativa⁶⁴. Asimismo, esta resolución puede ser cuestionada vía proceso contencioso administrativo ante el Poder Judicial, dentro del plazo de tres (3) meses posteriores a su notificación, de acuerdo con lo previsto en el numeral 1 del artículo 18 del Texto Único Ordenado la Ley N° 27584, Ley que regula el Proceso Contencioso Administrativo⁶⁵, aprobado por Decreto Supremo N° 011-2019-JUS.

Con la intervención de las señoras Comisionadas: Evelyn Edith Chumacero Asención, Erika Claudia Bedoya Chirinos, María de Fátima Ponce Regalado y Mónica Tatiana Siverio Puycan.

EVELYN EDITH CHUMACERO ASENCIÓN
Presidenta

⁶⁴ LEY 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicada el 2 de setiembre de 2010 y modificada por el DECRETO LEGISLATIVO 1308, publicado el 30 de diciembre de 2016

Artículo 125.- Competencia de los órganos resolutivos de procedimientos sumarísimos de protección al consumidor

(...)

La resolución que emita la correspondiente Comisión agota la vía administrativa y puede ser cuestionada mediante el proceso contencioso administrativo.

⁶⁵ TEXTO ÚNICO ORDENADO DE LA LEY 27584, LEY QUE REGULA EL PROCESO CONTENCIOSO ADMINISTRATIVO, aprobado por Decreto Supremo N° 011-2019-JUS, publicada el 4 de mayo de 2019

Artículo 18.- Plazos

La demanda deberá ser interpuesta dentro de los siguientes plazos:

(i) Cuando el objeto de la impugnación sean las actuaciones a que se refieren los numerales 1, 3, 4, 5 y 6 del Artículo 4 de esta Ley, el plazo será de tres meses a contar desde el conocimiento o notificación del acto material de impugnación, lo que ocurra primero.

(...)