PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE DERECHO

Informe Jurídico sobre la Resolución N°0364-2023/SPC-INDECOPI

Trabajo de Suficiencia Profesional para optar el Título de Abogada

Autora:

Kiara Miluska Durán Salcedo

Asesor:

Armando Rafel Prieto Hormaza

Lima, 2024

Informe de Similitud

Yo, PRIETO HORMAZA, ARMANDO RAFAEL, 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 N°0364-2023/SPC-INDECOPI”, del autor(a) DURAN SALCEDO, KIARA MILUSKA, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 25%. Así lo consigna el reporte de similitud emitido por el software Turnitin el 05/07/2024.

- 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, 10 de julio del 2024

PRIETO HORMAZA, ARMANDO RAFAEL	
DNI: 20054321	Firma: 
ORCID: https://orcid.org/0000-0003-3084-6149	

RESUMEN

En el presente Informe Jurídico, a propósito de la Resolución N°0364-2023/SPC-INDECOPI, se determinarán cuáles son las medidas de seguridad que una entidad bancaria debería adoptar ante operaciones no reconocidas entre cuentas propias realizadas por canal digital, para verificar que sí cumplió con su deber de idoneidad.

Al respecto, se concluirá que no corresponde que el sistema de monitoreo genere alerta ante transferencias entre cuentas propias, incluso si no pertenecen al patrón de consumo del cliente o si se efectúan entre cuentas de diferente moneda, ya que tal tipo de operaciones no son potencialmente fraudulentas al no dar indicios de que es un tercero quien podría está disponiendo de los fondos del titular de las cuentas, en tanto dichos fondos se mantienen dentro de la esfera de dominio del cliente.

Siendo ello así, ante un caso de transferencias no reconocidas entre cuentas propias por canal digital, para determinar que el Banco cumplió con su deber de idoneidad adoptando las medidas de seguridad aplicables, solo corresponde verificar que la entidad bancaria autorizó válidamente dichas operaciones conforme a la garantía legal respectiva, la cual dispone que las transferencias entre cuentas propias están exentas de la autenticación reforzada.

Tal exoneración se justifica en la naturaleza de las operaciones entre cuentas propias: no representan un posible fraude. De lo contrario, se les aplicaría la regla general que exige que las operaciones por canal digital estén sujetas a la autenticación reforzada.

Palabras clave

Medidas de seguridad, sistema de monitoreo, operaciones no reconocidas entre cuentas propias, operaciones potencialmente fraudulentas, exención de autenticación reforzada.

ABSTRACT

In this Legal Report, regarding Resolution N°0364-2023/SPC-INDECOPI, we will determine which are the security measures that a banking entity should adopt in the event of unrecognized transactions between its own accounts carried out through digital channels, in order to verify that the entity has complied with its duty of adequacy.

In this sense, it will be concluded that it is not appropriate for the monitoring system to generate an alert in the event of transfers between proprietary accounts, even if they do not belong to the customer's consumption pattern or if they are made between accounts of different currencies, since such transactions are not potentially fraudulent, since they do not give any indication that a third party could be disposing of the account holder's funds, since such funds remain within the customer's sphere of control.

This being so, in a case of unrecognized transfers between proprietary accounts by digital channel, in order to determine that the Bank complied with its duty of adequacy by adopting the applicable security measures, it is only necessary to verify that the banking entity validly authorized such operations in accordance with the respective legal guarantee, which provides that transfers between proprietary accounts are exempt from the reinforced authentication.

Such exemption is justified by the nature of the transactions between proprietary accounts: they do not represent a potential fraud. Otherwise, would apply to them the general rule requiring that digital channel transactions be subject to enhanced authentication.

Keywords

Security measures, monitoring system, unrecognized transactions between own accounts, potentially fraudulent transactions, enhanced authentication exemption.

ÍNDICE

PRINCIPALES DATOS DEL CASO

No. Exp. / No. Resolución o sentencia / Nombre del caso	Expediente N°0241-2021 / Resolución N°0364-2023/SPC-INDECOPI / Agurto VS BBVA
Áreas del derecho sobre las cuales versa el contenido del presente caso	Derecho del Consumidor y Derecho Bancario
Identificación de las resoluciones y sentencias más importantes	Resoluciones N°2063-2018/SPC-INDECOPI, N°2609-2022/SPC-INDECOPI, N°0318-2022/INDECOPI-CUS
Denunciante	JOSÉ ANTONIO AGURTO BELLOSO
Denunciado	BANCO BBVA PERÚ S.A.
Instancia administrativa	Sala Especializada en Protección al Consumidor

I. INTRODUCCIÓN

I.1. Justificación de la elección de la resolución

Una de las controversias más reclamadas y denunciadas por los consumidores bancarios son las operaciones no reconocidas. Al respecto, son dos (2) los principales temas que argumentan los clientes directa o indirectamente: la idoneidad del servicio que brinda la entidad bancaria y las medidas de seguridad que adoptó el Banco en relación a los consumos cuestionados.

En la gran mayoría de casos, las operaciones no reconocidas que se reclaman y denuncian son aquellas que implican que los fondos del cliente salen de su esfera de dominio, en tanto se han realizado retiros o Disposiciones de Efectivo, transferencias o pagos a terceros. También es usual que se reclame o denuncie que, luego del desembolso de un crédito no reconocido, se realizan las operaciones detalladas previamente.

En tal sentido, el caso materia de estudio es especial, porque el denunciante cuestiona únicamente operaciones efectuadas entre sus cuentas propias. Específicamente, son cuatro (4) transferencias realizadas desde la cuenta soles del denunciante hacia su cuenta dólares. Es así que este alega que el perjuicio habría sido ocasionado por el elevado tipo de cambio aplicado.

En ese orden de ideas, en el presente Informe Jurídico se precisará cuáles son las medidas de seguridad que una entidad bancaria debería adoptar ante operaciones no reconocidas entre cuentas propias realizadas por canal digital, para concluir que sí cumplió con su deber de idoneidad.

Para ello, primero, se detallará qué es el deber de idoneidad, en el marco de una relación de consumo bancaria. Segundo, se especificarán cuáles son las medidas de seguridad aplicables a las operaciones entre cuentas propias realizadas por canal digital, según el marco legal y criterios del Indecopi.

Tercero, se analizará si el cumplimiento del deber de idoneidad implica que el sistema de monitoreo genere alerta ante una operación entre cuentas propias de un monto mayor al importe máximo de una de las transacciones anteriores del cliente, y que se requiera la clave dinámica generada por el token, para confirmar dicho tipo de operación.

En este sentido, el presente trabajo es un aporte para determinar cuáles son las medidas de seguridad aplicables a las operaciones entre cuentas propias realizadas mediante canal digital.

I.2. Presentación del caso

La denuncia tramitada bajo el Expediente N°0241-2021/CPC-INDECOPI-CUS versa sobre cuatro (4) transferencias entre cuentas propias no reconocidas, realizadas desde el canal digital del denunciante, por la suma de S/31,000.00; las cuales le generaron el perjuicio de S/3,000.00 debido al tipo de cambio aplicado, pues se realizaron desde su cuenta de ahorro en soles hacia su cuenta de ahorro en dólares.

Al respecto, la Sala Especializada en Protección al Consumidor (en adelante, la Sala) revocó la Resolución N°0318-2022/INDECOPI-CUS emitida por la Comisión de la Oficina Regional del Indecopi de Cusco (en adelante, la Comisión) y declaró fundada la denuncia, pues concluyó que el denunciado no adoptó las medidas de seguridad correspondientes en relación a las cuatro (4) operaciones no reconocidas.

En atención a ello, en el presente informe se plantea como problema principal cuáles son las medidas de seguridad que una entidad bancaria debería adoptar ante operaciones no reconocidas entre cuentas propias realizadas por canal digital, para concluir que sí cumplió con su deber de idoneidad.

En esta línea, los problemas secundarios por abordar son (i) qué es el deber de idoneidad, en el marco de una relación de consumo bancaria; (ii) cuáles son las medidas de seguridad aplicables a las operaciones entre cuentas propias realizadas por canal digital, según el marco legal y criterios del Indecopi; y (iii) si el deber de idoneidad implica que el sistema de monitoreo genere alerta ante una operación entre cuentas propias de un monto mayor al importe máximo de una de las transacciones anteriores del cliente, y que el Banco requiera la clave dinámica generada por el token para confirmar dicho tipo de operación.

En este sentido, los principales instrumentos normativos que se emplearán en el presente informe son jurisprudencia relevante del Indecopi sobre medidas de seguridad así como la normativa pertinente: la Constitución Política del Perú de 1993 (en adelante, la Constitución), el Código de Protección y Defensa del Consumidor (en adelante, el Código de Consumo), el Reglamento de Tarjetas de Crédito y Débito (en adelante, el Reglamento de Tarjetas), y el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad (en adelante, el Reglamento de Ciberseguridad).

En atención al análisis a efectuar, se concluirá que, en el marco de operaciones entre cuentas propias por canal digital, para que el Banco brinde un servicio idóneo deberá cumplir con la medida de seguridad aplicable a dicho tipo de operación: la autorización válida aplicando la exención de la autenticación reforzada (garantía legal).

Es decir, no corresponde que el sistema de monitoreo identifique como posible fraude a las operaciones entre cuentas propias y, por ende, tampoco debe emitir ni gestionar alertas con respecto a estas; dado que, por las características de dichas operaciones, estas no dan indicios de que es un tercero quien podría estar efectuándolas sin la autorización del titular de la cuenta, por ende, no califican como operaciones potencialmente fraudulentas.

II. IDENTIFICACIÓN DE HECHOS RELEVANTES

II.1. Antecedentes

El 5 de agosto de 2021, el señor José Antonio Agurto Belloso (en adelante, el señor Agurto o el denunciante) recibió una llamada de un tercero, quien se presentó como funcionario del Banco BBVA Perú S.A (en adelante, el Banco BBVA o el denunciado) informándole sobre operaciones inusuales en diferentes comercios, entre ellos, Sura, Saga Falabella y Sodimac. Asimismo, le solicitó al señor Agurto que le brinde su Token Digital para proceder a anular dichas operaciones, a lo cual el denunciante no accedió.

En esa misma fecha, el señor Agurto se apersonó a una agencia del Banco BBVA para solicitar la cancelación de sus tarjetas. En ese momento, el denunciante notó que se habían realizado cuatro (4) transferencias no reconocidas por el monto total de S/31,000.00, desde su cuenta de ahorro en soles N°0011-****-****-0834 hacia su cuenta de ahorro en dólares N°0011-****-****-3831, conforme al siguiente detalle:

FECHA	HORA	CONCEPTO	IMPORTE
05/08/2021	17:31:20	Transferencia SAGAFALABELLA	S/ 3 500,00
	17:46:49		S/ 3 500,00
	17:55:11		S/ 10 000,00
	17:58:11	Transferencia SODIMAC	S/ 14 000,00

Al respecto, el señor Agurto precisó que, si bien los fondos se encontraban en su cuenta de ahorro en dólares, sufrió un perjuicio económico de S/3,000.00 debido al tipo de cambio aplicado (S/4.50).

II.2. Hechos relevantes del caso

A continuación, se presentarán los hechos relevantes del caso materia de análisis, tramitado bajo el Expediente N°0241-2021/CPC-INDECOPI-CUS

Primera Instancia

1. El 23 de setiembre de 2021, el señor Agurto presentó una denuncia contra el Banco BBVA, ante la Comisión, indicando no reconocer cuatro (4) transferencias por la suma de S/31,000.00, efectuadas el 05 de setiembre de 2021, desde su cuenta de ahorro en soles N°0011-****-****-0834 hacia su cuenta de ahorro en dólares N°0011-****-****-3831.

2. El 01 de diciembre de 2021, la Secretaría Técnica de la Comisión de la Oficina Regional del Indecopi de Cusco (en adelante, la Secretaría Técnica) admitió a trámite la denuncia por la presunta infracción al artículo 19° del Código de Consumo, pues el Banco no habría adoptado las medidas de seguridad en relación a las cuatro (4) operaciones no reconocidas.

3. El 30 de diciembre de 2021, el denunciado presentó sus descargos, alegando lo siguiente:

- Las cuatro (4) operaciones no reconocidas por el denunciante se efectuaron válidamente mediante la Banca por Internet.
- Presentó el reporte “Log de Operaciones KT80”, donde se evidenciaba el ingreso al canal digital previo a cada operación cuestionada, así como los registros de las confirmaciones de estas.
- Por ejemplo, sobre la primera (1°) operación, señaló que de dicha reportería se evidencia que (i) el 5 de agosto de 2021 a las 17:31:19 horas hubo un ingreso a la Banca por Internet, lo cual queda acreditado bajo la glosa “J2A1”, para lo cual se requirió la clave de la Banca por Internet. Además, (ii) que a las 17:31:20 horas se concretó con éxito la primera Transferencia entre Cuentas Propias, lo cual queda acreditado bajo la glosa “Cod. Estado=S”, siendo que la glosa “BQ46” refiere a que la operación es una Transferencia entre Cuentas Propias.

4. El 01 de febrero de 2022, el señor Agurto presentó un escrito complementario señalando que la suma de las operaciones cuestionadas supera el límite para transferencias que establece el Banco BBVA (S/3,000.00).

5. El 26 de mayo de 2022, la Comisión emitió la Resolución N°0318-2022/INDECOPI-CUS, en la cual realizó el siguiente análisis:

(i) Sobre el deber de monitoreo del Banco BBVA

- Las Transferencias entre Cuentas Propias no son consideradas inusuales porque los fondos no salen de la esfera del titular. Por lo tanto, no correspondía que el Banco BBVA emitiera alguna alerta por las operaciones; ni que realice el bloqueo preventivo de la tarjeta de débito del cliente.

(ii) Sobre la validez de las operaciones cuestionadas

- De la revisión de la reportería presentada por el Banco BBVA, se verificó que las operaciones no reconocidas por el cliente son Transferencias entre Cuentas Propias (glosa “BQ46”), las cuales fueron realizadas exitosamente (glosa COD_ESTADO= “S”), previo ingreso al canal digital haciendo uso de datos de conocimiento exclusivo del titular. Asimismo, para ese tipo de operaciones no corresponde la generación ni uso de la clave dinámica.

6. En este orden de ideas, la Comisión declaró infundada la denuncia, ya que el denunciado acreditó que adoptó las medidas de seguridad correspondientes respecto a las cuatro (4) operaciones reclamadas. En efecto, denegó la medida correctiva solicitada, así como el pago de costos y costas del procedimiento.

7. El 18 de junio de 2022, el señor Agurto apeló la resolución de la Comisión señalando que las operaciones cuestionadas debieron generar alerta considerando que desde hace dos (2) años no efectúa alguna operación mayor o igual a S/31,000.00.

Segunda Instancia

8. El 8 de febrero de 2023, la Sala emitió la Resolución N°0364-2023/SPC-INDECOPI, mediante la cual realizó el siguiente análisis:

(i) Sobre el deber de monitoreo del Banco BBVA

- La Sala precisó que, de la revisión de los movimientos de la cuenta de ahorro en soles N°0011-****-****-0834 del periodo marzo a julio 2021, se verificó que el comportamiento de consumo del denunciante era el siguiente:

Periodo de facturación	Cantidad de operaciones	Operación individual de mayor valor	Monto total consumido por periodo	Cantidad de consumos máxima por día
31/03/2021	1	S/ 97,50	S/ 97,50	1
30/04/2021	-	-	-	-
30/05/2021	-	-	-	-
30/06/2021	-	-	-	-
30/07/2021	**17**	**S/ 2 800,00**	**S/ 14 824,10**	**5**

- En atención a ello, la Sala concluyó que la primera (1°) operación cuestionada, de importe de S/3,500.00, debió ser detectada como inusual por el sistema de monitoreo del Banco BBVA toda vez que, como máximo, el denunciante realizó con anterioridad una (1) operación del monto de S/2,800.00; es decir, por un importe menor al de la operación no reconocida referida.

- En ese sentido, la Sala señaló que el sistema de monitoreo debió generar una alerta una vez procesada la primera (1°) operación, y atenderla, evitando que se realicen las tres (3) operaciones posteriores.

(ii) Sobre la validez de las operaciones

- Sin perjuicio de lo anterior, la Sala destacó que la reportería (Log de Operaciones KT80) presentada por el denunciado no generaba convicción sobre la válida autorización de las operaciones materia de denuncia porque figuraba como cuentas de origen y de destino, cuentas de ahorro diferentes a las indicadas por el denunciante.

9. Así pues, la Sala revocó la Resolución N°0318-2022/INDECOPI-CUS, y declaró fundada la denuncia por infracción del artículo 19° del Código de Consumo, toda vez que el denunciado no adoptó las medidas de seguridad correspondientes, en relación a las cuatro (4) operaciones no reconocidas.

   En este sentido, la Sala ordenó al Banco BBVA como medida correctiva anular las cuatro (4) operaciones reclamadas, reintegrando el monto total de S/31,000.00 en la cuenta de ahorro en soles N°0011-****-****-0834 del cliente. Asimismo, la Sala ordenó el pago de costas y de costos, de corresponder; y le impuso la multa final 11,60 UIT.

III. IDENTIFICACIÓN DE LOS PRINCIPALES PROBLEMAS JURÍDICOS

III.1. Problema principal

¿Cuáles son las medidas de seguridad que una entidad bancaria debería adoptar ante operaciones no reconocidas entre cuentas propias realizadas por canal digital, para concluir que sí cumplió con su deber de idoneidad?

III.2. Problemas secundarios

1. ¿Qué es el deber de idoneidad, en el marco de una relación de consumo bancaria?
2. ¿Cuáles son las medidas de seguridad aplicables a las operaciones entre cuentas propias efectuadas por canal digital, según el marco legal y criterios del Indecopi?
3. ¿El cumplimiento del deber de idoneidad implica que el sistema de monitoreo genere alerta ante una operación entre cuentas propias de un monto mayor al importe máximo de una de las transacciones anteriores del cliente, y que el Banco requiera la clave dinámica generada por el token para confirmar dicho tipo de operación?

IV. POSICIÓN DE LA CANDIDATA

IV.1. Respuestas preliminares a los problemas secundarios

Problema secundario 1: ¿Qué es el deber de idoneidad, en el marco de una relación de consumo bancaria?

De acuerdo al artículo 65° de la Constitución, el Estado garantiza la defensa de los consumidores. En el numeral 1 del artículo IV del Código de Consumo se describe los caracteres que debe tener un consumidor para ser considerado como tal. Ahora bien, se reconoce que los proveedores deben cumplir con el deber de idoneidad, el cual es abordado en los artículos 18° y 19° del Código de Consumo.

A mayor abundamiento, en el artículo 20° del Código de Consumo se establece que, para verificar la idoneidad del servicio o producto otorgado, se debe evidenciar que el proveedor cumplió con las garantías legales, explícitas e implícitas.

En virtud a lo señalado, en una relación de consumo bancaria, el consumidor es el cliente financiero, mientras que el proveedor es la entidad financiera. En ese sentido, el servicio que este último brinde debe ser idóneo. Para ello, deberá cumplir con las garantías correspondientes.

Problema secundario 2: ¿Cuáles son las medidas de seguridad aplicables a las operaciones entre cuentas propias efectuadas por canal digital, según el marco legal y criterios del Indecopi?

Ante un caso de operaciones no reconocidas, es responsabilidad de las entidades financieras acreditar que las operaciones fueron debidamente autenticadas y registradas (artículo 23° del Reglamento de Tarjetas) de acuerdo a las medidas de seguridad correspondientes.

Al respecto, en el artículo 17° de dicho Reglamento se especifican las medidas de seguridad que las entidades deben adoptar como mínimo respecto al monitoreo de operaciones: deben contar con un sistema de monitoreo que identifique operaciones inusuales, considerando el patrón de consumo del cliente; generar alerta por estas; y gestionar dichas alertas oportunamente.

Por otro lado, en el Reglamento de Ciberseguridad se desarrollan las medidas de seguridad que las entidades financieras deben adoptar en relación a la autenticación del cliente. Cabe señalar que, según el literal c) del artículo 2 de tal Reglamento, la autenticación es el proceso mediante el cual se valida la identidad del usuario requiriéndole el “uso de las credenciales que se le asignan”. La autenticación puede estar compuesta por uno “o más factores […] independientes".

De acuerdo al literal j) del artículo 2° del cuerpo normativo referido, los factores de autenticación tienen tres (3) categorías: “algo que solo el usuario conoce, algo que solo el usuario posee [o] algo que el usuario es, que incluye las características biométricas”.

Así pues, en el artículo 19° del Reglamento de Ciberseguridad se establece que las entidades financieras deben contar con una autenticación reforzada para las operaciones que se realicen por canal digital, a efectos de evitar operaciones fraudulentas como las que “que impliquen pagos o transferencia de fondos a terceros”.

No obstante, mediante el literal b) del numeral 1) del artículo 20° del Reglamento de Ciberseguridad se exonera de la autenticación reforzada a las operaciones entre cuentas propias.

Ahora bien, se debe considerar que una operación posiblemente fraudulenta es aquella que da indicios de que un tercero está realizándola sin la autorización del titular de la cuenta. Dicho tercero, o, mejor dicho, el delincuente, buscará un beneficio económico propio e inmediato extrayendo la mayor cantidad de fondos del cliente en el menor tiempo posible.

En virtud a ello, las transferencias entre cuentas propias, incluso siendo estas de diferente moneda, no son operaciones potencialmente fraudulentas en tanto no representan las características necesarias para suponer que es un tercero quien podría estar realizándolas en perjuicio del cliente, debido a que los fondos no salen de la esfera de dominio del cliente.

Siendo ello así, lo que justifica que las operaciones entre cuentas propias estén exentas de la autenticación reforzada es precisamente que no representan un posible fraude. De lo contrario, estarían sujetas a la regla general recogida en el artículo 19° del Reglamento de Ciberseguridad: autenticación reforzada.

En resumen, para concluir que la entidad financiera cumplió con las medidas de seguridad respecto a transferencias no reconocidas entre cuentas propias por canal digital, no corresponde analizar si el sistema de monitoreo debió generar alerta con respecto a dicho tipo de operaciones dado que, por su naturaleza, no son potencialmente fraudulentas.

Así pues, solo se deberá corroborar que el Banco cumplió con autorizarlas válidamente exonerándolas de la autenticación reforzada, lo cual es una garantía legal.

Problema secundario 3: ¿El cumplimiento del deber de idoneidad implica que el sistema de monitoreo genere alerta ante una operación entre cuentas propias de un monto mayor al importe máximo de una de las transacciones anteriores del cliente, y que el Banco requiera la clave dinámica generada por el token para confirmar dicho tipo de operación?

El cumplimiento del deber de idoneidad de la entidad financiera, en el marco de un caso de operaciones no reconocidas, implica el cumplimiento de las medidas de seguridad, las cuales suponen de manera conjunta (i) el deber de monitoreo y (ii) la válida autorización de las operaciones.

Ahora bien, no corresponde que el sistema de monitoreo genere alerta respecto a las operaciones entre cuentas propias realizadas por canal digital, debido a la naturaleza de estas: no son potencialmente fraudulentas ni inusuales. Esto aplica independientemente de si las cuentas entre las que se realiza la transferencia son de diferente moneda o si el importe de la operación es mayor al monto máximo de una de las transacciones previas del cliente.

Por otro lado, para que el Banco autorice válidamente las operaciones entre cuentas propias, que se efectúen por canal digital, deberá hacerlo conforme a lo dispuesto en la garantía legal pertinente (literal b) del numeral 1) del artículo 20° del Reglamento de Ciberseguridad); es decir, aplicando la exención de la autenticación reforzada, lo cual supone que no se requiera la clave dinámica generada por el token para confirmar la operación.

En tal sentido, ante un caso de transferencias no reconocidas entre cuentas propias, para determinar que el Banco adoptó las medidas de seguridad, solo

corresponde verificar que autorizó válidamente las operaciones de acuerdo a la garantía legal.

IV.2. Posición individual sobre el fallo de la resolución

La Sala revocó la Resolución emitida de la Comisión y declaró fundada la denuncia pues el Banco BBVA no adoptó las medidas de seguridad necesarias en relación a las cuatro (4) operaciones no reconocidas entre cuentas propias.

Sobre ello, estoy de acuerdo con el dictamen de la Sala, pero no comparto los motivos que expone en su Resolución N°0364-2023/SPC-INDECOPI respecto al deber de monitoreo del Banco ante operaciones no reconocidas entre cuentas propias.

Primero, es relevante precisar que, en general, el cumplimiento de las medidas de seguridad implica, de manera conjunta, que el Banco haya actuado conforme a su deber de monitoreo y que haya autorizado válidamente las operaciones. La entidad financiera debe cumplir necesariamente con ambos para determinar que actuó conforme a las medidas de seguridad exigidas.

Si bien la Sala aplicó este criterio general al caso en concreto, lo cierto es que, considerando que son operaciones entre cuentas propias, esto no sería lo adecuado, pues no corresponde exigir que el sistema de monitoreo genere alerta con respecto a estas, incluso si son operaciones entre cuentas de diferente moneda y si no están dentro del patrón de consumo del cliente; ya que dichas operaciones no son potencialmente fraudulentas.

Las transferencias entre cuentas propias no representan un posible fraude, ya que no dan indicios de que es un tercero quien está disponiendo de los fondos del cliente sin su consentimiento; toda vez que el delincuente no podría lograr su objetivo -obtener un beneficio económico propio e inmediato-, en tanto los fondos no salen de la esfera de dominio del cliente.

En efecto, en el caso en concreto, no correspondía que el sistema de monitoreo genere alerta por alguna de las operaciones entre cuentas propias. Por el contrario, solo correspondía verificar si el Banco cumplió con autorizarlas válidamente conforme al mecanismo de autenticación exigido por la garantía legal recogida en el literal b) del numeral 1) del artículo 20° del Reglamento de Ciberseguridad.

En tal sentido, se debió desestimar el argumento del cliente, mediante el cual señala que las operaciones cuestionadas serían inusuales, ya que no efectúa operaciones por un monto mayor o igual a S/31,000.00 – que es la suma de las operaciones cuestionadas-, desde hace dos (2) años.

Ahora bien, respecto a la validez de las operaciones materia de análisis, cabe destacar que de acuerdo a artículo 23° del Reglamento de Tarjetas, es responsabilidad de las entidades financieras acreditar que las operaciones no reconocidas fueron debidamente autenticadas y registradas según las medidas de seguridad correspondientes.

Bajo esta línea, en el presente caso, el Banco debió demostrar que autorizó las transferencias entre cuentas propias sin aplicar la autenticación reforzada. Al respecto, tal como indica la Sala, los reportes presentados por el Banco para acreditar la validez de las operaciones no generan convicción; ya que, hay una discordancia entre los números de cuentas que figuran en el reporte y los que el cliente indica en su denuncia; por lo que no es un medio probatorio fehaciente.

Por otro lado, cabe precisar que las medidas de seguridad que el Banco debe adoptar no están definidas de forma exclusiva por las bases legales correspondientes (garantía legal); sino también por las garantías explícitas, esto es, aquello a lo que se obliga la entidad bancaria más allá de lo que se indica en la norma.

En relación a las operaciones por canal digital, una garantía explícita es el límite monetario por transacción o diario. El Banco informa a los clientes sobre cuál es el importe máximo que puede, por ejemplo, transferir en una operación, siendo dicho tope configurable por el cliente bajo ciertas condiciones. Por lo tanto, cuando el Banco autoriza una operación, esta debe estar dentro de los límites configurados.

Así pues, en el presente caso, las operaciones cuestionadas fueron realizadas en un día por el importe total de S/31,000.00. Sobre ello, es importante destacar que el denunciado no establece de manera predeterminada un límite monetario en relación a las operaciones entre cuentas propias; y tampoco ofrece la opción de que sus clientes configuren un tope monetario para dicho tipo de transacciones.

Por lo tanto, era oportuno que la Sala desestime el argumento del cliente sobre que las operaciones no reconocidas habrían superado el monto máximo permitido por el Banco para realizar transferencias entre cuentas propias.

En conclusión, en el presente caso, si bien la denuncia correspondía ser declarada fundada, el fundamento debió ser que el Banco no acreditó fehacientemente haber autorizado válidamente las cuatro (4) operaciones reclamadas.

Bajo esta línea, la medida correctiva ordenada por la Sala fue la correcta: reintegrar el monto total de las operaciones cuestionadas (S/31,000.00) en la cuenta de ahorro en soles N°0011-****-****-0834 del denunciante, pues el denunciado no acreditó la validez de estas.

V. ANÁLISIS DE LOS PROBLEMAS JURÍDICOS

Problema secundario 1: ¿Qué es el deber de idoneidad, en el marco de una relación de consumo bancaria?

El mercado es la interacción entre la oferta y la demanda, es decir, hay presencia innata de las relaciones de consumo, en las cuales, hay un proveedor y un consumidor. La oferta de bienes y servicios está sustentada en la demanda de este último.

Así pues, el consumidor es clave para el funcionamiento del mercado. “El mercado existe por y para los consumidores […]. Protegiendo a los consumidores, se podrá llegar al buen funcionamiento de mercado y al bienestar de la sociedad” (Indecopi, 2000, en Salas Valderrama, R. A, 2010, p.183).

En este sentido, mediante el artículo 65° de la Constitución se reconoce que el Estado vela por la defensa de los consumidores garantizando su derecho a la información sobre los bienes y servicios que se ofertan en el mercado.

Ahora bien, conforme al numeral 1 del artículo IV del Código de Consumo, los consumidores son las “personas naturales o jurídicas que adquieren, utilizan o disfrutan como destinatarios finales productos o servicios […] para beneficio propio o de su grupo familiar o social”, no actuando como parte de una “actividad empresarial o profesional”.

También son consumidores los microempresarios que evidencien “asimetría informativa con el proveedor”. En caso de duda, se considerará consumidor a quien “adquiere, usa o disfruta” un producto o servicio.

Por otro lado, los proveedores tienen que cumplir con su deber de idoneidad ante los consumidores, el cual es definido mediante el artículo 18° del Código de Consumo, bajo los siguientes términos:

> *“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.

La idoneidad es evaluada en función a la propia naturaleza del producto o servicio y a su aptitud para satisfacer la finalidad para la cual ha sido puesto en el mercado"

En el artículo 19° del Código de Consumo se señala que "el proveedor responde por la idoneidad y calidad de los productos y servicios ofrecidos". Es decir, la idoneidad es la correlación entre lo que el consumidor efectivamente recibe por parte del proveedor y la expectativa del consumidor originada por las características de la oferta del proveedor. Este último tiene que cumplir con su deber de idoneidad, y de no hacerlo asumirá responsabilidad administrativa.

Ahora bien, en el artículo 20° del Código de Consumo se indica que "para determinar la idoneidad de un producto o servicio, debe compararse el mismo con las garantías que el proveedor está brindando y a las que está obligado". Según lo dispuesto en dicho artículo, las garantías son las características o condiciones del producto o servicio, las cuales pueden ser legales, explícitas o implícitas.

Una garantía legal refiere a cuando una disposición normativa exige su cumplimiento para poder prestar un servicio o comercializar un producto. En efecto, se presupone que forma parte del contenido del contrato de relación de consumo; que no es posible pacto en contrario; y que no "puede ser desplazada por una garantía explícita ni por una implícita".

Una garantía explícita es aquella que se desprende de un "medio por el que se pruebe específicamente lo ofrecido al consumidor", como, por ejemplo, los términos y condiciones de un servicio. Esta garantía prima sobre una garantía implícita.

Por otro lado, una garantía será implícita cuando, ante la no existencia de una garantía legal o explícita, se concluya que, el producto o servicio “debe atenderse a los fines y usos previsibles para un consumidor”, conforme al caso en particular, así como a los usos y costumbres (Rodríguez García G. M., 2014, p.308).

En este orden de ideas, en una relación de consumo bancaria, el proveedor del servicio financiero es el Banco, mientras que el consumidor es el cliente. Siendo ello así, cuando los consumidores financieros presentan sus denuncias por operaciones no reconocidas ante el Indecopi, este analizará si el Banco cumplió con su deber de idoneidad en el caso en concreto.

Es decir, la autoridad determinará si el servicio financiero brindado por el Banco se efectuó cumpliendo con las garantías legales, explícitas y/o implícitas, según corresponda.

A mayor abundamiento, cabe indicar que un ejemplo de garantía legal son las medidas de seguridad recogidas en el Reglamento de Tarjetas y en el Reglamento de Ciberseguridad (deber de monitoreo y válida autorización de operaciones), las cuales el Banco debe adoptar necesariamente con respecto a las operaciones que realicen sus clientes, según corresponda.

En cambio, una garantía explícita son los términos de una campaña particular para ganar puntos o millas; o los límites establecidos por el Banco para realizar determinadas operaciones, los pueden ser modificados por los clientes sujetándose a las condiciones que establezca el Banco.

En conclusión, en una relación de consumo bancaria, el deber de idoneidad implica que el Banco, como proveedor, brinde el servicio financiero de acuerdo a las garantías aplicables al caso en concreto.

Problema secundario 2: ¿Cuáles son las medidas de seguridad aplicables a las operaciones entre cuentas propias efectuadas por canal digital, según el marco legal y criterios del Indecopi?

Uno de los cuerpos normativos más relevantes en el marco de operaciones no reconocidas, es el Reglamento de Tarjetas, el cual, de acuerdo a sus considerandos, recoge disposiciones sobre las siguientes materias:

> *"[…] condiciones contractuales, remisión de información y medidas de seguridad aplicables, con especial énfasis en la verificación de la identidad del titular o usuario y el establecimiento de límites de responsabilidad en el uso fraudulento de dichas tarjetas".*

En tal sentido, de acuerdo al artículo 23° del Reglamento de Tarjetas, ante un caso de operaciones no reconocidas, las entidades financieras tienen la responsabilidad de acreditar que aquellas "fueron [debidamente] autenticadas y registradas", de acuerdo a las medidas de seguridad correspondientes.

Sin embargo, si el Banco demostrara ello, pero se presentara alguno de los supuestos expuestos en la base legal referida, la entidad bancaria igual deberá asumir la responsabilidad. Por ejemplo, ante operaciones de micropago o pago rápido, el usuario no asumirá responsabilidad por dicho tipo de operación, sino el Banco.

Ahora bien, en el artículo 17° del Reglamento de Tarjetas, se detallan las medidas de seguridad que deben, como mínimo, adoptar las entidades financieras respecto al monitoreo de las operaciones que realicen los usuarios: deben tener un sistema de monitoreo de operaciones que identifique las operaciones que no guardan relación con el "comportamiento habitual de consumo del usuario" o que representen un "patrón de fraude", el cual será advertido en base a un análisis de la "información histórica de las operaciones" del usuario.

Ante una operación inusual, el sistema de monitoreo debe generar una alerta oportuna, la cual deberá ser atendida mediante acciones que eviten que se realicen posteriormente más operaciones fraudulentas. Por ejemplo, se debe optar el bloqueo de la tarjeta de crédito o débito, de los canales digitales del cliente, entre otros.

En ese sentido, en el artículo 22° del Reglamento de Tarjetas, se indica que ante operaciones que pueden representar un patrón de fraude, el procedimiento del Banco debe contar con los siguientes dos (2) elementos mínimos: comunicación inmediata al cliente sobre las operaciones, y efectuar el bloqueo "temporal o definitivo de la tarjeta".

Por otro lado, en el Reglamento de Ciberseguridad se desarrollan los lineamientos de los mecanismos de autenticación de usuarios, que deben implementar dichas entidades para autorizar válidamente las operaciones que aquellos realicen.

Así pues, es importante partir por entender qué es la autenticación y cuáles son los factores de autenticación de usuarios. De acuerdo al literal c) del artículo 2 del Reglamento de Ciberseguridad, la autenticación "es el proceso que permite verificar" la identidad del usuario requiriéndole el "uso de las credenciales que se le asignan". La autenticación puede estar compuesta por uno "o más factores […] independientes".

Según el literal j) del artículo 2 del cuerpo normativo referido, los factores de autenticación de usuario son aquellos cuya finalidad es validar "la identidad de un usuario", y que corresponden a tres (3) categorías: "algo que solo el usuario conoce, algo que solo el usuario posee [o] algo que el usuario es, que incluye las características biométricas".

En atención a lo expuesto, el artículo 19° del Reglamento de Ciberseguridad dispone que las entidades financieras deben implementar una "autenticación

reforzada para operaciones por canal digital", para evitar la realización de "operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente, como las operaciones […] que impliquen […] transferencia de fondos a terceros". Para una autenticación reforzada, el proveedor financiero deberá:

> *"a) Utilizar una combinación de factores de autenticación, […] que, por lo menos, correspondan a dos categorías distintas* [referidas en el literal j) del artículo 2] *y que sean independientes uno del otro.*
> *b) Contar con un control ante ataques de hombre en el medio, que puede incluir un código único generado 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."*

En otras palabras, para las operaciones por canal digital, la entidad financiera debe implementar una autenticación reforzada la cual consiste en (i) el inicio de sesión en el canal digital previo a las operaciones solicitando el ingreso de una contraseña o de identificación con recursos biométricos, por ejemplo, TouchiD o FaceiD; (ii) la generación de una clave dinámica por un Token Digital o Físico; (iii) y el empleo de esa clave dinámica para la confirmación final de la operación.

Sin embargo, en el numeral 1) del artículo 20° del Reglamento de Ciberseguridad se precisa que determinadas operaciones por canal digital "están exentas del requisito de autenticación reforzada indicado en el artículo 19° […], a excepción del indicado en el literal c)". Dentro de ellas, se encuentran las transferencias entre cuentas propias de persona natural o jurídica, "*siempre que dichas cuentas se mantengan en la misma empresa".*

A mayor abundamiento, cabe identificar de qué manera el Indecopi aplica la normativa expuesta en su análisis de denuncias por operaciones no reconocidas en general. En las Resoluciones N°2063-2018/SPC-INDECPI y N°2609-2022/SPC-INDECOPI, el Indecopi realizó un cambio de criterio sobre el análisis

del (i) cumplimiento de la adopción de medidas de seguridad por parte de la entidad financiera, y (ii) del patrón de consumo, en el marco de operaciones no reconocidas.

Anteriormente, en los casos de denuncias por operaciones no reconocidas, tanto la imputación de cargos como el análisis de la controversia eran sobre dos (2) hechos individuales: la autorización válida de las operaciones cuestionadas, y el correcto funcionamiento del sistema de monitoreo ante tales operaciones (Fundamentos 9-10 de la Resolución N°2063-2018/SPC-INDECOPI).

Sin embargo, en la Resolución N°2063-2018/ SPC-INDECOPI, la Sala realizó un análisis sistemático de los artículos 15°, 16° y 17° del Reglamento de Tarjetas, concluyendo que, para determinar que la entidad financiera cumplió con adoptar las medidas de seguridad exigidas, se debe verificar de manera conjunta si la entidad, mediante su sistema de monitoreo, cumplió con (i) validar si la operación era inusual por no concordar con el patrón de consumo del titular del producto con cargo al cual se efectuaron las operaciones inusuales, (ii) generar alerta oportuna en caso se tratase de una operación fraudulenta, y (iii) tomar acción para evitar que se realicen operaciones inusuales posteriores, por ejemplo, bloqueando el producto (Fundamentos 14 y 16).

Asimismo, también precisó que se debe verificar si la entidad autorizó válidamente la operación, de acuerdo a los mecanismos de autenticación respectivos para identificar al titular del producto, como, por ejemplo, la lectura de tarjeta chip e ingreso de clave; ya que ello forma parte de las medidas de seguridad que la entidad tiene que adoptar (Fundamentos 14-15).

En este orden de ideas, la Sala concluyó que el análisis descrito debe realizarse “dentro de un mismo tipo infractor”, el cual versa sobre la adopción de medidas de seguridad respecto a las operaciones no reconocidas. Esto independientemente de si, en el marco de una denuncia de operaciones no

reconocidas, los denunciantes cuestionan solo la validez de la operación, o solo las medidas de seguridad o monitoreo adoptadas (Fundamentos 18-19).

Por otro lado, en la Resolución N°2609-2022/SPC-INDECOPI, la Sala especificó que el patrón de consumo será determinado en cada caso considerando el comportamiento respectivo de los denunciantes; por lo que no se puede establecer de manera predeterminada que cierto tipo de operación será irregular para todos los usuarios. Es decir, la Sala concluyó que el patrón de consumo tiene una “naturaleza personalísima” (Fundamento 48).

En esta línea, la Sala determinó que para identificar el patrón de consumo del titular del producto con cargo al cual se hicieron operaciones no reconocidas se tiene que determinar el monto de las operaciones que el denunciante usualmente efectúa con cargo a dicho producto, independientemente del canal o frecuencia, en atención a la revisión de los estados o movimientos de cuenta correspondientes (Fundamentos 50-52).

Cabe indicar que el canal o frecuencia de los consumos no pueden determinar de manera independiente que este sea inusual, sino que deben ser analizados junto con el importe de las operaciones que usualmente realiza el denunciante (Fundamento 53).

En resumen, en general, las medidas de seguridad hacen referencia de manera conjunta (i) al deber de monitoreo del Banco, es decir, a que implemente un sistema de monitoreo que identifique operaciones fraudulentas considerando el patrón de consumo de cliente, emita alertas por ellas y las gestione evitando operaciones inusuales posteriores; y (ii) a los mecanismos o factores de autenticación que el Banco debe aplicar para verificar la identidad del cliente y, así, autorizar válidamente las operaciones. Dicha autenticación será o no reforzada según el tipo de operación que se efectúe.

En tal sentido, en el marco de un caso de operaciones no reconocidas en general, si la entidad financiera no cumple con su deber de monitoreo y/o con autorizar válidamente las operaciones de acuerdo a los mecanismos correspondientes, habrá incumplido con adoptar las medidas de seguridad exigidas.

Ahora bien, cabe indicar que el sistema de monitoreo de las entidades financieras no es predictivo ni preventivo. Es decir, solo podrá identificar una operación inusual al comportamiento habitual del cliente una vez realizada dicha operación.

Por lo tanto, en caso corresponda la emisión de una alerta y, en consecuencia, la gestión de esta -por ejemplo, bloqueando la tarjeta de débito-, estas acciones serán tomadas luego de efectuada la operación que ameritó la generación de una alerta, con el fin de evitar que se realicen posteriormente más operaciones fraudulentas.

A continuación, se identificarán cuáles son las medidas de seguridad aplicables a las operaciones entre cuentas propias en específico. Sin embargo, primero, es importante tomar en consideración que las operaciones entre cuentas propias no son potencialmente fraudulentas.

Las operaciones que representan un posible fraude son aquellas que otorguen indicios de que un tercero está disponiendo de los fondos del cliente sin su autorización, causándole como consecuencia un perjuicio económico. El objetivo de dicho tercero es extraer la mayor cantidad de fondos del cliente en el menor tiempo posible.

Es decir, dicho tercero buscará un beneficio inmediato propio como resultado de tales operaciones que realice. ¿Qué provecho obtendría un delincuente al hacer transferencias entre las cuentas propias de su víctima? Ninguno, porque los fondos siguen bajo el dominio del titular de las cuentas.

Si bien las operaciones entre cuentas propias implican un cargo en la cuenta de origen del cliente, los fondos se mantienen disponibles dentro de su esfera de dominio. Es decir, el cliente podrá disponer de tales fondos, ya que la cuenta de destino es también suya y fue contratada con el mismo Banco en el que se mantiene la cuenta de origen.

En virtud a lo mencionado, las operaciones entre cuentas propias no representan un posible fraude ya que no reúnen las características necesarias para dar indicios de que es un tercero quien esté realizándolas sin la autorización del cliente.

Así pues, por un lado, de acuerdo al literal b) del numeral 1) del artículo 20° del Reglamento de Ciberseguridad, las operaciones entre cuentas propias están exentas de la autenticación reforzada. Lo que justifica que este tipo de operaciones estén exoneradas de la autenticación reforzada es precisamente la naturaleza de aquellas: no representan un posible fraude ni son inusuales.

En caso se considerase que las transferencias entre cuentas propias podrían representan un riesgo de fraude, estas estarían sujetas a la regla general recogida en el artículo 19° del Reglamento de Ciberseguridad: aplicación de la autenticación reforzada.

El literal b) del numeral 1) del artículo 20° del Reglamento de Ciberseguridad recoge la garantía legal referida a la válida autorización de las transacciones entre cuentas propias.

Por ejemplo, si un usuario quiere realizar una transferencia entre sus cuentas propias, que mantiene con una misma entidad bancaria, desde su canal digital, deberá ingresar a este haciendo uso de su contraseña o mediante la autenticación con biometría.

Luego, podrá efectuar la operación sin que se le solicite el ingreso previo de la clave dinámica generada por el Token, ya que, para este tipo de transacción, no se requiere la generación ni uso de dicha clave. Si bajo esos parámetros el Banco autoriza la operación, entonces lo habrá hecho válidamente cumpliendo con la garantía legal antes descrita, pues no aplicó la autenticación reforzada.

Por otro lado, no corresponde exigir al Banco ejecutar su deber de monitoreo respecto a las operaciones entre cuentas propias. Es decir, el sistema de monitoreo no debe identificar a dichas operaciones como inusuales, tampoco debe generar una alerta ni gestionarla, dada la naturaleza de las transferencias entre cuentas propias: no son potencialmente fraudulentas.

A mayor abundamiento, cabe identificar algunos de los principales motivos por los cuales un consumidor realiza operaciones entre sus cuentas propias, a efectos de evidenciar que son transacciones usuales en su comportamiento de consumo y, en consecuencia, cuáles serían los riesgos de considerarlas como operaciones que pueden ser materializaciones de posibles fraudes.

Por un lado, algunas de las principales motivaciones de los consumidores para recurrir a operaciones entre cuentas propias de una misma entidad bancaria son las siguientes: trasladar sus fondos a otra cuenta suya por una cuestión de organización de finanzas, porque su cuenta propia beneficiaria de la transferencia le ofrece realizar determinadas operaciones sin el cobro de comisiones o le brinda mayores beneficios.

Asimismo, los clientes no solo hacen operaciones entre sus cuentas propias que tengan una misma moneda, por ejemplo, podrían querer realizar la compra de moneda extranjera a efectos de disponer de sus fondos en una moneda diferente a la nacional.

Basta con que nos preguntemos “¿cuántas transferencias entre cuentas propias realizo al día o semana?”, para identificar que el realizar transferencias entre cuentas propias es muy común en el comportamiento de los consumidores.

En virtud a lo mencionado, no es inusual que un consumidor efectúe transferencias entre sus cuentas propias, independientemente del monto y la moneda de las operaciones, en el transcurso de un día, e incluso pueden hacerlas con pocos minutos de diferencia entre cada una.

Cabe anotar que los consumidores no toman especial atención a la frecuencia con la cual hacen operaciones entre sus cuentas propias ni al importe de estas, ya que este tipo de operaciones no están sujetas al cobro de alguna comisión; pues los fondos se trasladan entre las cuentas que el cliente mantiene en un mismo Banco.

El único costo en el que podrían incurrir los clientes es el tipo de cambio al hacer una transferencia entre sus cuentas sus cuentas propias cuyas monedas sean distintas. Al respecto, se podría plantear como contraargumento que, bajo este supuesto, las operaciones entre cuentas propias sí deberían ser consideradas como potencialmente fraudulentas, porque pueden generar un perjuicio económico al titular de las cuentas.

No obstante, no comparto dicho criterio, ya que incluso cuando se hacen transferencias entre cuentas propias de moneda diferente, estas operaciones no representan un posible fraude, considerando que la probabilidad de que sea un delincuente quien esté realizando este tipo de transacción es totalmente mínima, pues dicho tercero no podría conseguir su objetivo: un beneficio económico inmediato y propio, en tanto no puede verse beneficiado por el tipo de cambio que se cobre por hacer tales transferencias.

Además, se debe evaluar el impacto que tendría en el mercado el hecho de que las operaciones entre cuentas propias sean consideradas por el sistema de

monitoreo como potencialmente fraudulentas, tomando en cuenta que se estaría generalizando el único supuesto en el cual el titular de las cuentas podría verse afectado económicamente -el cobro de tipo de cambio por operaciones no reconocidas entre cuentas propias de diferente moneda-, y que la probabilidad de que un consumidor se vea ante esta situación es muy baja. Si los Bancos adoptaran esta medida, los estragos los impactarían a ellos y a los consumidores.

Así pues, considerando que los fondos se mantienen en la esfera económica del titular de las cuentas propias, sería ineficiente para el cliente que dichas transacciones sean consideradas como riesgosas, porque tendrían que reflexionar innecesariamente si mover o no sus fondos y por cuánto monto hacerlo, pues, de lo contrario, se arriesgarían a que el sistema de monitoreo del Banco alerte por dicha operación y que, como consecuencia, bloquee sus cuentas de ahorro, su tarjeta de débito e incluso sus canales digitales.

Este supuesto negado, implica que los clientes tengan que asumir costos transaccionales innecesarios, ya que deberán comunicarse con el Banco para informar que sí fueron ellos los que hicieron las operaciones entre cuentas propias, pese a que los fondos se han movido solo dentro de su esfera y que, por tanto, deberían poder disponer de ellos sin inconveniente.

Además, para que las entidades bancarias implementen en su sistema de monitoreo el factor de identificar que las operaciones entre cuentas propias son potencialmente fraudulentas, tendrían que asumir costos transaccionales que, de una u otra forma, serían trasladados a los consumidores, viéndose perjudicados de otra manera más.

En efecto, catalogar a las operaciones entre cuentas propias como operaciones potencialmente fraudulentas generaría que se restrinja las posibilidades de los consumidores de trasladar sus fondos entre sus cuentas, de acuerdo a las necesidades e intereses que tengan, sin preocuparse por el monto que están

transfiriendo o por la cantidad de veces seguidas que están haciendo ese tipo de operación durante el día.

En atención a lo desarrollado, no corresponde que el sistema de monitoreo del Banco identifique a las operaciones entre cuentas propias como posiblemente fraudulentas, tampoco generar ni gestionar una alerta respecto a ellas, ya que dichas operaciones no representan un riesgo de fraude en tanto no dan indicios de que es un tercero quien está disponiendo de los fondos del cliente sin su consentimiento.

En efecto, para determinar que el Banco cumplió con aplicar las medidas de seguridad correspondientes respecto a operaciones no reconocidas entre cuentas propias por canal digital, basta con validar que fueron debidamente autorizadas aplicando la exención de la atención reforzada.

Problema secundario 3: ¿El cumplimiento del deber de idoneidad implica que el sistema de monitoreo genere alerta ante una operación entre cuentas propias de un monto mayor al importe máximo de una de las transacciones anteriores del cliente, y que el Banco requiera la clave dinámica generada por el token para confirmar dicho tipo de operación?

El deber de idoneidad en el marco de una relación de consumo bancaria supone que el servicio otorgado por la entidad financiera se haya realizado de acuerdo a las garantías legales, explícitas o implícitas, según corresponda.

En tal sentido, ante un caso de operaciones no reconocidas entre cuentas propias realizadas por canal digital, para verificar que el Banco cumplió con brindar un servicio idóneo, se tendrá que determinar que adoptó las medidas de seguridad correspondientes.

Conforme a lo detallado anteriormente, no corresponde que el sistema de monitoreo identifique como potencialmente fraudulentas a las operaciones entre

cuentas propias. Esto aplica incluso si las cuentas propias son de monedas diferentes y hay un cobro de tipo de cambio de por medio; y/o si la transferencia entre cuentas propias es de un monto mayor al importe máximo de una de las transacciones anteriores del cliente.

Esto porque solo las operaciones que reúnen características de ser fraudulentas o inusuales son las que deben generar alerta en el sistema. Sin embargo, las operaciones entre cuentas propias no cuentan con dicha característica de posible fraude, porque no dan indicios de que es un tercero quien esté realizándolas sin la autorización del titular de las cuentas.

Ahora bien, aplicando lo expuesto al caso materia de análisis del presente Informe Jurídico, donde el cliente cuestiona cuatro (4) operaciones no reconocidas entre cuentas propias de diferente moneda, se concluye que, contrariamente a lo indicado por la Sala en la Resolución N°0364-2023/SPC-INDECOPI, no correspondía que el sistema de monitoreo genere alerta por alguna de las transferencias, independientemente de si estas guardaban o no relación con el patrón de consumo del cliente.

Por otro lado, en cuanto a la autorización válida de las operaciones entre cuentas propias, conforme a lo expuesto anteriormente, la garantía legal refiere que dichas operaciones están exentas de la autenticación reforzada (literal b) del numeral 1) del artículo 20° del Reglamento de Ciberseguridad).

Así pues, para que el Banco cumpla con su deber de idoneidad, en relación a operaciones entre cuentas propias realizadas por canal digital, no deberá solicitar la generación y uso de una clave dinámica. Es decir, solo tendrá que requerir el ingreso previo al canal digital utilizando la clave secreta respectiva.

Asimismo, cabe traer a colación el artículo 23° del Reglamento de Tarjetas, mediante el cual se establece que, en el marco de operaciones no reconocidas, las entidades financieras tienen que demostrar que las autorizaron conforme a

los mecanismos de seguridad respectivos. Es decir, recae sobre ellas la carga de la prueba.

En tal sentido, en el presente caso el Banco debió acreditar que autorizó las cuatro (4) operaciones no reconocidas válidamente, aplicando la exención de autenticación reforzada. Es decir, debió sustentar fehacientemente el ingreso previo exitoso al canal digital del cliente utilizando la contraseña correspondiente; y la confirmación de las cuatro (4) operaciones sin el requerimiento previo de la generación y uso de la clave dinámica generada por el token.

No obstante, tal como señala la Sala en la Resolución N°0364-2023/SPC-INDECOPI, la entidad financiera no demostró que autorizó válidamente las operaciones materia de controversia, ya que la reportería que presentó no generó convicción, pues figuraban números de cuentas de origen y de destino que no coincidían con los señalados por el cliente; y el Banco no esclareció dicha contradicción.

Ahora bien, ya que las medidas de seguridad implican, de manera conjunta, (i) el deber de monitoreo y (ii) la válida autorización de las operaciones; si el Banco no cumple con ambos o uno de ellos, incurre en el incumplimiento de adopción de medidas de seguridad. En efecto, incumple con su deber de idoneidad; ya que dichas medidas de seguridad son garantías legales.

Por lo tanto, en el presente caso, se concluye que el Banco no aplicó las medidas de seguridad correspondientes respecto a las cuatro (4) operaciones reclamadas, ya que no acreditó fehacientemente haberlas autorizado válidamente.

En atención a ello, si bien concuerdo con el dictamen de la Sala de declarar fundada la denuncia, considero que no correspondía analizar si el caso en concreto el sistema de monitoreo debió generar alerta por las operaciones no reconocidas, pues conforme a lo desarrollado en puntos anteriores, la naturaleza

de las transferencias entre cuentas propias es no ser potencialmente fraudulentas ni inusuales.

VI. CONCLUSIONES

1. La entidad bancaria cumplirá con su deber de idoneidad cuando el servicio financiero sea brindado de acuerdo a las garantías legales, explícitas o implícitas, según corresponda. Así pues, ante un caso de operaciones no reconocidas, para determinar que el Banco brindó un servicio idóneo, se deberá verificar que cumplió con la garantía legal de adoptar las medidas de seguridad aplicables (deber de monitoreo y autorización válida de las operaciones), así como si cumplió con las garantías explícitas correspondientes.

2. La naturaleza de las operaciones entre cuentas propias es no ser potencialmente fraudulentas, en tanto no dan indicios de que un tercero las estaría realizando sin autorización del cliente, ya que dicho tercero no podría cometer su objetivo -obtener un beneficio económico propio e inmediato-, pues los fondos se mantienen dentro de la esfera de dominio del cliente. Esto aplica incluso si se realizan transferencias entre cuentas propias de diferente moneda.

   Así pues, por un lado, de acuerdo al literal b) del numeral 1) del artículo 20° del Reglamento de Ciberseguridad, las operaciones entre cuentas propias están exentas de la autenticación reforzada (garantía legal). La justificación para que este tipo de operaciones estén exentas de la autenticación reforzada es precisamente su naturaleza: no representan un posible fraude ni son inusuales.

   Por otro lado, no corresponde que el sistema de monitoreo identifique a las operaciones entre cuentas propias como potencialmente fraudulentas, incluso si se tratan de cuentas de diferente moneda; ya que tales transacciones no representan dicho riesgo en tanto no reúnen las

características necesarias para dar indicios de que es un tercero quien está realizándolas en perjuicio del titular de las cuentas.

3. Frente a un caso de operaciones no reconocidas entre cuentas propias por canal digital, el cumplimiento del deber de idoneidad por parte del Banco estará determinado por la verificación de que autorizó válidamente tales operaciones aplicando la exención de la autenticación reforzada.

   Ahora bien, considerando que las transferencias entre cuentas propias no son potencialmente fraudulentas, no corresponde que el sistema de monitoreo considere que dicho tipo de operaciones representan un posible fraude y que, por ende, emita una alerta.

   Ello aplica independientemente de si las operaciones se efectúan entre cuentas de diferente moneda, y/o si el importe de la transferencia es mayor al monto máximo de una de las transacciones anteriores del cliente.

   Siendo ello así, considerando que en el presente caso el Banco no acreditó fehacientemente haber autorizado válidamente las operaciones no reconocidas, correspondía declarar fundada la denuncia.

BIBLIOGRAFÍA

Doctrina

Rodríguez García, G. M. (2014). El apogeo y decadencia del deber de idoneidad en la jurisprudencia peruana de protección al consumidor. *THEMIS Revista De Derecho, 65,* 303-314. https://revistas.pucp.edu.pe/index.php/themis/article/view/10876

Salas Valderrama, R. A. (2010). Algunos apuntes y reflexiones sobre la Tutela de los derechos de los consumidores y la Asimetría Informativa en el

mercado. *Foro Jurídico*, (11), 182-193. https://revistas.pucp.edu.pe/index.php/forojuridico/article/view/18587

Jurisprudencia

- Sala Especializada en Protección al Consumidor de Indecopi. Resolución N°2063-2018/SPC-INDECOPI (2018).
- Sala Especializada en Protección al Consumidor de Indecopi. Resolución N°2609-2022/SPC-INDECOPI (2022).

Normativa

- Constitución Política del Perú, 29 de diciembre de 1993.
- Código de Protección y Defensa del Consumidor, Ley Nº29571, Diario Oficial El Peruano, 01 de setiembre de 2010.
- Reglamento de Tarjetas de Crédito y Débito, Superintendencia de Banca, Seguros y AFP, Resolución S.B.S. N°6523-2013, 30 de octubre de 2013.
- Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, Superintendencia de Banca, Seguros y AFP, Resolución S.B.S. Nº504-2021, 19 de febrero de 2021.

PROCEDENCIA	**:**	COMISIÓN DE LA OFICINA REGIONAL DEL INDECOPI DE CUSCO
PROCEDIMIENTO	**:**	DE PARTE
DENUNCIANTE	**:**	JOSÉ ANTONIO AGURTO BELLOSO
DENUNCIADO	**:**	BANCO BBVA PERÚ S.A.
MATERIAS	**:**	SERVICIOS FINANCIEROS DEBER DE IDONEIDAD
ACTIVIDAD	**:**	OTROS TIPOS DE INTERMEDIACIÓN MONETARIA

SUMILLA: Se revoca la Resolución 0318-2022/INDECOPI-CUS que declaró infundada la denuncia interpuesta contra Banco BBVA Perú S.A.; y, en consecuencia, se declara fundada la misma, por infracción del artículo 19° de la Ley 29571, Código de Protección y Defensa del Consumidor, al haberse verificado que no adoptó las medidas de seguridad necesarias en el procesamiento de cuatro (4) operaciones no reconocidas, consistentes en transferencias por el importe total de S/ 31 000,00 desde su cuenta en soles a su cuenta en dólares.

SANCIÓN: 11,60 UIT

Lima, 8 de febrero de 2023

ANTECEDENTES

1. Mediante escrito del 23 de setiembre de 2021, complementado con escrito del 15 de octubre de ese mismo año, el señor José Antonio Agurto Belloso (en adelante, el señor Agurto) denunció a Banco BBVA Perú S.A. (en adelante, el Banco), ante la Comisión de la Oficina Regional del Indecopi de Cusco (en adelante, la Comisión), por presunta infracción de la Ley 29571, Código de Protección y Defensa del Consumidor (en adelante, el Código), manifestando lo siguiente:

   (i) Adquirió del denunciado la Cuenta en Soles 0011-****-****-0834 y la Cuenta en Dólares 0011-****-****-3831;
   (ii) el 5 de agosto de 2021, recibió una llamada telefónica de una persona que se identificó como trabajador del Banco, indicándole de la realización de consumos inusuales en Sura, Saga Falabella, Sodimac y otros comercios; no obstante, pese a que dicha persona le solicitó información sobre su token digital, no se la brindó;
   (iii) ese mismo día, se acercó inmediatamente a la agencia bancaria para solicitar la anulación de sus tarjetas, tomando conocimiento además que se habían realizado transferencias de dinero por el importe total de S/ 31 000,00 de su cuenta en soles a su cuenta en dólares;
   (iv) pese a que dicha suma de dinero se encontraba dentro de su cuenta bancaria, lo cierto es que a esta le fue aplicada un tipo de cambio de S/

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

4,50 (cuya conversión fue a US$ 7 099,17), lo que le generó una pérdida de S/ 3 000,00;

(v) en atención a ello, presentó dos (2) reclamos ante el libro de reclamaciones del denunciado, los cuales fueron atendidos por este con una respuesta desfavorable; y,

(vi) solicitó como medida correctiva que el Banco cumpliera con extornar la operación controvertida a su cuenta en soles; asimismo, solicitó el pago de las costas y los costos del procedimiento.

2. El 30 de diciembre de 2021, el Banco presentó sus descargos, aseverando lo siguiente:

(i) El señor Agurto no había cumplido con acreditar su cuestionamiento, por lo que no se le podía atribuir responsabilidad en base a meras afirmaciones;

(ii) la operación controvertida fue realizada válidamente a través de la banca por internet con el ingreso de información sensible y confidencial que solo tenía el denunciante;

(iii) la medida de seguridad que utilizaba era el protocolo Secure Socket Layer (SSL), a través del cual la información entre su banca por internet – móvil y la computadora o dispositivo del cliente viajaba de forma cifrada; siendo que su aplicativo móvil estaba siendo constantemente actualizado para satisfacción de sus clientes;

(iv) el denunciante se encontraba afiliado al token digital desde el 10 de octubre de 2019, para lo cual este consignó el número telefónico 984***431, el cual inclusive fue proporcionado en su denuncia;

(v) el código de cliente del señor Agurto era 23802865, asimismo, su código de token digital era BB-04-RP0400102900, siendo este único por cliente;

(vi) la validez de la primera operación cuestionada quedó registrada en el reporte denominado “Log de Operaciones KT80”, en donde se apreciaba que, el 5 de agosto de 2021 a las 17:31:19 horas, se registró el ingreso correcto a la Banca GNET (J2A1) con el uso correcto de la clave, registrándose la operación de manera satisfactoria a las 17:31:20 horas;

(vii) de igual modo, a efectos de acreditar la validez de las otras operaciones cuestionadas, presentaba los reportes denominados “Log de Operaciones KT80” respectivos;

(viii) dado que las operaciones antes señaladas fueron transferidas entre las propias cuentas del señor Agurto, no se requirió la clave token digital, información que fue consignada en los reportes con el comando BQ46; y,

(ix) al momento en que las operaciones no reconocidas fueron realizadas, la tarjeta del denunciante estuvo activa, siendo esta bloqueada recién el 5 de agosto de 2021 a las 18:02:00.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

3. El 1 de febrero de 2022, el señor Agurto presentó un escrito, señalando, entre otros puntos, que no era razonable que: (i) si la entidad bancaria solo le permitía transferir montos máximos de S/ 3 000,00, haya permitido que se realice una transferencia de S/ 31 000,00 en un solo día; y, (ii) el concepto de las transferencias efectuadas entre sus propias cuentas fue de "Sura, Saga Falabella, Sodimac y otros".

4. El 12 de mayo de 2022, la Secretaría Técnica de la Comisión de la Oficina Regional del Indecopi de Cusco (en adelante, la Secretaría Técnica de la Comisión) emitió el Informe Final de Instrucción 0071-2022/CPC-INDECOPI-CUS, a través del cual brindó recomendaciones a la Comisión sobre el hecho materia de denuncia, el mismo que fue oportunamente trasladado a las partes para que presenten sus observaciones.

5. El 20 de mayo de 2022, el señor Agurto presentó un escrito, reiterando su posición sobre el hecho denunciado contra el Banco, así como negando los argumentos expuestos por este.

6. Mediante Resolución 0318-2022/INDECOPI-CUS del 26 de mayo de 2022, la Comisión emitió el siguiente pronunciamiento:

   (i) Declaró infundada la denuncia interpuesta por el señor Agurto contra el Banco, por presunta infracción del artículo 19° del Código, al haberse verificado que adoptó las medidas de seguridad necesarias en el procesamiento de las cuatro (4) operaciones no reconocidas, consistentes en transferencias por el importe total de S/ 31 000,00, desde su cuenta en soles a su cuenta en dólares;
   (ii) denegó las medidas correctivas y el pago de las costas y los costos del procedimiento solicitados por el señor Agurto.

7. El 18 de junio de 2022, el señor Agurto presentó su recurso de apelación contra la resolución antes señalada, indicando lo siguiente:

   (i) El Banco no había implementado las medidas de seguridad necesarias para identificar un patrón de fraude; asimismo, tampoco había monitoreado correctamente su comportamiento habitual de consumo pues, desde hace dos (2) años, no realizaba ninguna operación mayor o igual a S/ 31 000,00 menos aún en un solo día, debiéndose haber generado alguna alerta para constatar si era él quien efectuaba las operaciones no reconocidas;
   (ii) no se había tomado en consideración que el denunciado no presentó descargos sobre el hecho de que él no proporcionó a ninguna persona el token digital, motivo por el cual su dinero no fue sustraído de su cuenta bancaria por terceras personas;

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

(iii) su disconformidad consistía en la pérdida de dinero que sufrió por la conversión al tipo de cambio de soles a dólares, puesto que dicha operación no fue realizada por él;
(iv) no era razonable que, si la entidad bancaria solo le permitía transferir montos máximos de S/ 3 000,00, haya permitido que se realice una transferencia de S/ 31 000,00 en un solo día, lo que demostraba que su sistema de seguridad era ineficiente pues era el denunciado quien debía acreditar la autorización de dicha operación;
(v) ante su cuestionamiento de que no era regular que las transferencias materia de controversia hayan sido denominadas "Sura, Saga Falabella, Sodimac y otros" pese a que, supuestamente, estas se trataban de transferencias entre sus propias cuentas, la Comisión señaló indebidamente que el Banco no estaba obligado a presentar su defensa respecto de ello, en tanto, no era una imputación de cargos; y,
(vi) ante ello, no se estaba tomando en cuenta que no tenía recursos para ser asesorado por un estudio jurídico, así como tampoco la afectación económica del hecho infractor denunciado.

8. El 22 de setiembre de 2022, el señor Agurto presentó un escrito, solicitando que se convoque a una audiencia de conciliación. Cabe precisar que, dicha solicitud fue traslada al Banco mediante Proveído 2 del 20 de diciembre de 2022, acto administrativo que le fue notificado el 29 de diciembre de 2022.

9. Por su parte, el 4 de enero de 2023, el Banco presentó un escrito, indicando que no era necesario que se lleve a cabo la audiencia de conciliación solicitada por el denunciante.

ANÁLISIS

Cuestión previa: Sobre la solicitud de una audiencia de conciliación

10. El artículo VI del Título Preliminar del Código establece como política pública del Estado la promoción del uso de los mecanismos alternativos de solución de controversias, tales como el sistema de arbitraje de consumo, la mediación y la conciliación antes e incluso durante la tramitación del procedimiento administrativo[1]. En esa línea, el artículo 29° del Decreto Legislativo 807, Ley sobre Facultades, Normas y Organización del Indecopi[2], señala que la citación

[1] **LEY 29571. CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR. TÍTULO PRELIMINAR. Artículo VI. - Políticas públicas.** El Estado garantiza mecanismos eficaces y expeditivos para la solución de conflictos entre proveedores y consumidores. Para tal efecto, promueve que los proveedores atiendan y solucionen directa y rápidamente los reclamos de los consumidores, el uso de mecanismos alternativos de solución como la mediación, la conciliación y el arbitraje de consumo voluntario, y sistemas de autorregulación; asimismo, garantiza el acceso a procedimientos administrativos y judiciales ágiles, expeditos y eficaces para la resolución de conflictos y la reparación de daños. Igualmente, facilita el acceso a las acciones por intereses colectivos y difusos.

[2] **DECRETO LEGISLATIVO 807. LEY SOBRE FACULTADES, NORMAS Y ORGANIZACIÓN DEL INDECOPI. Artículo 29º.-** En cualquier estado del procedimiento, e incluso antes de admitirse a trámite la denuncia, el Secretario

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

a una audiencia de conciliación constituye una facultad de la autoridad administrativa, quien en el ejercicio de su discrecionalidad podrá disponer su realización o denegarla.

11. Como puede apreciarse, la citación a una audiencia de conciliación es una facultad discrecional de la Administración, siendo que dicha actuación, al ser de carácter facultativo, no obliga a la autoridad de consumo a convocar a las partes a la referida diligencia.

12. De los actuados, se advierte que, ante esta instancia, mediante escrito presentado el 22 de setiembre de 2022, el señor Agurto solicitó que se convoque a las partes a una audiencia de conciliación. No obstante, conviene tener en cuenta que, si bien mediante Proveído 2 del 20 de diciembre de 2022 esta Sala puso en conocimiento del Banco el pedido del denunciante para programar una audiencia de conciliación, el denunciado manifestó su intención de no conciliar.

13. Por consiguiente, considerando que de los actuados no se desprende un ánimo conciliatorio por parte del Banco, ni ningún otro elemento o circunstancia que justifique convocar a una audiencia de conciliación, corresponde denegar el pedido del señor Agurto.

Sobre el deber de idoneidad

14. El artículo 18° del Código dispone que la idoneidad debe ser entendida como la correspondencia entre lo que el consumidor espera y lo que efectivamente recibe, en función a lo que se le hubiera ofrecido, la publicidad e información transmitida, entre otros factores, atendiendo a las circunstancias del caso. A su vez, el artículo 19° del citado Código indica que el proveedor responde por la idoneidad y calidad de los productos y servicios ofrecidos[3].

Técnico podrá citar a las partes a audiencia de conciliación. La audiencia se desarrollará ante el Secretario Técnico o ante la persona que éste designe. Si ambas partes arribaran a un acuerdo respecto de la denuncia, se levantará un acta donde conste el acuerdo respectivo, el mismo que tendrá efectos de transacción extrajudicial. El cualquier caso, la Comisión podrá continuar de oficio el procedimiento, si del análisis de los hechos denunciados considera que podría estarse afectando intereses de terceros.

[3] **LEY 29571. CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR. Artículo 18º.- 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.
La idoneidad es evaluada en función a la propia naturaleza del producto o servicio y a su aptitud para satisfacer la finalidad para la cual ha sido puesto en el mercado.
Las autorizaciones por parte de los organismos del Estado para la fabricación de un producto o la prestación de un servicio, en los casos que sea necesario, no eximen de responsabilidad al proveedor frente al consumidor.
(…)

Artículo 19º.- 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 éstos, así como por el contenido y la vida útil del producto indicado en el envase, en lo que corresponda.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

15. En aplicación de esta norma, los proveedores tienen el deber de brindar los productos y servicios ofrecidos en las condiciones acordadas o en las condiciones que resulten previsibles, atendiendo a la naturaleza y circunstancias que rodean la adquisición del producto o la prestación del servicio, así como a la normatividad que rige su prestación.

16. En el presente caso, el señor Agurto denunció que el Banco no habría adoptado las medidas de seguridad respectivas pues habría permitido el procesamiento de cuatro (4) operaciones no reconocidas, por el importe total de S/ 31 000,00 desde su cuenta en soles a su cuenta en dólares, conforme al siguiente detalle:

FECHA	HORA	CONCEPTO	IMPORTE
05/08/2021	17:31:20	Transferencia SAGAFALABELLA	S/ 3 500,00
	17:46:49		S/ 3 500,00
	17:55:11		S/ 10 000,00
	17:58:11	Transferencia SODIMAC	S/ 14 000,00

17. Al respecto, la Comisión declaró infundada la denuncia interpuesta contra el Banco, por presunta infracción del artículo 19° del Código, puesto que se verificó que las operaciones controvertidas fueron efectuadas válidamente desde la cuenta en soles a la cuenta en dólares del denunciante, las cuales se encontraban dentro del comportamiento habitual de consumo.

18. Dado el recurso de apelación formulado por el señor Agurto y en aras de dilucidar la responsabilidad del Banco, corresponde verificar, en primer lugar, si dicha entidad cumplió con su deber de monitoreo y detección de operaciones inusuales o sospechosas a efectos de determinar si correspondía generar una alerta; así, una vez superada dicha evaluación, se procederá a analizar si se realizó un cargo justificado de la misma, cumpliendo con los requisitos de validez pertinentes.

Sobre el comportamiento habitual de consumo del señor Agurto

19. De acuerdo con la garantía legal contemplada en el artículo 17º del Reglamento de Tarjetas de Crédito y Débito (en adelante, el Reglamento), aprobado por Resolución SBS 6523-2013, el parámetro de idoneidad en la prestación de servicios y productos financieros en el marco de la afectación de las cuentas o líneas de crédito de los consumidores, se encuentra comprendido -de forma unívoca- por las medidas de seguridad atribuidas a las entidades financieras por la normativa sectorial, encontrándose entre ellas, el deber de monitoreo y detección de consumos inusuales o sospechosos.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

20. Bajo este orden de ideas, las expectativas razonables de un consumidor, al contar con un producto financiero con las entidades financieras, importan que estas desplieguen **todas** las medidas de seguridad contempladas a su cargo legalmente (sin excepción alguna), siendo que, la falta de observancia de una de ellas comportaría la prestación de un servicio financiero inidóneo.

21. Siendo esto así, incluso si un consumidor no manifiesta su disconformidad con la conducta de su contraparte, en lo concerniente al deber de monitoreo de operaciones contemplado en el artículo 17° del Reglamento, corresponde a la autoridad evaluar el cumplimiento de dicha garantía legal, al constituir parte del cumplimiento del deber de idoneidad en virtud de las medidas de seguridad adoptadas por el proveedor frente a la transacción cuestionada.

22. En ese sentido, más allá del formato de redacción que un consumidor pueda utilizar en su denuncia o el tenor de la misma, se entiende que cuando este cuestiona ante la Administración el cargo de un consumo no reconocido, lo hace con el fin de que se verifique que la entidad financiera adoptó **todas las medidas de seguridad a las que se encontraba obligada**, motivo por el cual es necesario realizar un análisis conjunto de tales medidas de seguridad, hayan sido, o no, expresamente invocadas por la denunciante.

23. Habiéndose aclarado dicho punto, conviene puntualizar que no resulta un hecho controvertido que la Cuenta en Soles 0011-****-****-0834 y la Cuenta en Dólares 0011-****-****-3831 se encontraban activas en la oportunidad en que se efectuaron las operaciones cuestionadas (5 de agosto de 2021).

24. Ahora bien, el artículo 2°.5 del Reglamento define que el comportamiento habitual de consumo del usuario se refiere al tipo de operaciones que usualmente realiza cada uno con sus tarjetas, considerando diversos factores: el país de consumo, tipos de comercio, frecuencia, canal utilizado, entre otros, los cuales pueden ser determinados a partir de la información histórica de las operaciones de cada usuario que registra la empresa.

25. Al respecto, el artículo 17° del Reglamento, establece lo siguiente:

> *"**Artículo 17°. - Medidas de seguridad respecto al monitoreo y realización de las operaciones***
> *Las empresas deben adoptar como mínimo las siguientes medidas de seguridad con respecto a las operaciones con tarjetas que realizan los usuarios:*
> *1. Contar con sistemas de monitoreo de operaciones, que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual de consumo del usuario.*
> *2. Implementar procedimientos complementarios para gestionar las alertas generadas por el sistema de monitoreo de operaciones.*

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

3. Identificar patrones de fraude, mediante el análisis sistemático de la información histórica de las operaciones, los que deberán incorporarse al sistema de monitoreo de operaciones (…)". [Sic]

26. Conforme al artículo citado previamente, se desprende que las empresas del sistema financiero deben adoptar como medidas de seguridad, entre otras, la implementación de sistemas de monitoreo de operaciones, que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual de consumo del usuario.

27. Así, la finalidad del artículo 17° del Reglamento descansa en la protección de los usuarios frente al cargo de transacciones fraudulentas en las cuentas de sus tarjetas de crédito o débito, a partir de, entre otros aspectos, la revisión del movimiento histórico de transacciones en las respectivas cuentas, lo cual evidentemente involucra el análisis de operaciones que permitan a la empresa supervisada generar razonablemente un patrón de consumo respecto al uso de dicho producto por parte de su cliente.

28. Como se aprecia, la normativa sectorial exige que el historial de consumo que las entidades del sistema financiero construyan respecto a cada uno de sus clientes, e integrarlo a su sistema de monitoreo, debe responder a una serie de factores que la entidad bancaria o financiera determine a partir del análisis sistemático de la información histórica del usuario.

29. Al respecto, este Colegiado considera que, a efectos de determinar el comportamiento habitual de un consumidor, se debe tener en cuenta que la formación de dicho patrón responde a aspectos individuales de cada cliente, su modo de consumo, entre otras características de naturaleza personalísima, por lo que no es posible concluir que el procesamiento de una operación con características específicas sea inusual para todos los consumidores.

30. En atención a lo referido, es necesario precisar los alcances del criterio aplicable a los casos vinculados a denuncias por falta de adopción de medidas de seguridad ante la ejecución de operaciones no reconocidas por los usuarios de servicios financieros, a fin de revestir de un contenido más completo a la determinación del comportamiento habitual de cada cliente.

31. Así, a manera de otorgar un criterio objetivo a la determinación del comportamiento habitual de consumo de un denunciante, se deberá tener en cuenta el importe individual de las operaciones que el consumidor usualmente realizaba con el producto objeto de denuncia, lo cual será obtenido del estudio de los estados de cuenta o estado de saldos de movimientos previamente emitidos, correspondientes a las líneas de crédito y/o cuentas objeto de estudio.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

32. En esa línea, la conclusión de si una operación es inusual o no al comportamiento habitual de consumo del consumidor deberá realizarse teniendo en cuenta si, de manera previa a su ejecución, el interesado había realizado, con cargo al producto estudiado, operaciones por importes similares a los controvertidos en sede administrativa.

33. Es pertinente acotar que el estudio referido previamente debe comprender un análisis que considere la totalidad de canales utilizados previamente por el consumidor, no restringiendo su consideración (es decir, el importe de la operación estudiada) a un canal específico y/o a una frecuencia de uso específica, por cuanto la naturaleza del producto financiero (salvo pacto en contrario) no limita su uso a determinados canales y/o en determinada frecuencia.

34. En ese sentido, si bien la frecuencia con la que se realizan las operaciones y los canales por los cuales estas se ejecutan, entre otras características, son elementos importantes de la conformación del patrón de consumo del cliente, lo cierto es que tales elementos diferenciadores, por sí solos, no puede llevar a determinar -inequívocamente- que una operación es inusual o sospechosa, por lo que tales factores deberán ser analizados en conjunto con la información obtenida del historial de consumos del cliente, referida al importe de las operaciones que usualmente realizaba. A manera de ejemplo, no sería posible concluir que una operación es inusual o sospechosa únicamente porque se realizó -por primera vez- en un establecimiento nuevo o en una frecuencia distinta a la fijada en periodos previos, debiendo considerarse en tales casos, si el monto individual de la operación que estamos estudiando es uno que se encuentra dentro del rango de montos que el cliente usualmente consumía con cargo a su línea de crédito o fondos de cuentas.

35. En este punto es pertinente dejar constancia que el análisis fijado previamente es uno a efectos de detectar si una operación, procesada en la cuenta de la denunciante, presentaba características inusuales al comportamiento habitual de consumo del cliente que ameritasen que el Banco la detecte como inusual y/o sospechosa, en atención a su deber de monitoreo, pero que no implica de modo alguno el desconocimiento de la existencia de autorizaciones y/o habilitaciones previas que necesitan ser otorgadas a efectos de procesar determinadas operaciones, siendo que -en tales casos- no estamos ante la ejecución de una operación inusual, sino ante la realización de una operación que no tenía autorización de ser procesada.

36. En ese orden de ideas, de la revisión de los Estados de Movimientos vinculados a la Cuenta en Soles 0011-****-****-0834[4], correspondientes

[4] Ver de la foja 10 a la foja 14 del expediente.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

únicamente a los meses de marzo y julio de 2021, meses previos en que se ejecutaron las transacciones no reconocidas, se colige lo siguiente:

Periodo de facturación	Cantidad de operaciones	Operación individual de mayor valor	Monto total consumido por periodo	Cantidad de consumos máxima por día
31/03/2021	1	S/ 97,50	S/ 97,50	1
30/04/2021	-	-	-	-
30/05/2021	-	-	-	-
30/06/2021	-	-	-	-
30/07/2021	**17**	**S/ 2 800,00**	**S/ 14 824,10**	**5**

37. Atendiendo a lo indicado, esta Sala verifica que la primera (1º) operación -por S/ 3 500,00- excedió el importe máximo por consumo individual registrado previamente por el consumidor, ascendente a S/ 2 800,00. En tal sentido, el Banco se encontraba obligado a identificar esta operación como inusual al patrón de consumo fijado en el párrafo previo y, como consecuencia, adoptar medidas de seguridad conducentes a evitar el uso continuado del producto financiero materia de análisis.

38. Cabe señalar que, si la entidad financiera hubiera cumplido con su deber de monitoreo adecuadamente, hubiera podido detectar la primera transacción como inusual, alertar a la consumidora y haber adoptado mecanismos oportunos, como el bloqueo de la cuenta de ahorros de la denunciante, que -en su conjunto- hubieran evitado que se procesen operaciones adicionales en perjuicio de su cliente.

39. Sin embargo, no ha quedado acreditado que la entidad financiera haya cumplido con la invocada obligación, pues permitió que luego de la operación detallada se efectuaran tres (3) operaciones adicionales que nunca debieron siquiera procesarse, al haber sucedido a una operación que debió levantar una alerta de consumo, por lo que corresponde atribuirle responsabilidad.

40. Sin perjuicio de lo mencionado, es menester evaluar si la transacción sospechosa -que debió generar una alerta en los sistemas del proveedor- fue procesada en cumplimiento de los requisitos de validez necesarios, pues, para que tal operación haya podido levantar la alerta correspondiente, esta debió haber sido previamente procesado por la entidad financiera en su sistema, por cuanto el sistema de monitoreo del Banco no es uno de naturaleza predictivo, sino que se construye con cada operación efectuada por cada consumidor.

41. Al respecto, corresponde indicar que, a criterio de este Colegiado, las medidas de seguridad a las que se encuentra sujeta la entidad financiera implican el monitoreo de las operaciones del cliente, a efectos de que -ante la ejecución

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

de una operación- la entidad financiera pueda identificar la ocurrencia de una acción inusual y/o posiblemente fraudulenta y, así, desplegar acciones inmediatas con el fin de mitigar las consecuencias negativas derivadas de dicha acción. En esa línea, las medidas dispuestas no contemplan que la operación ajena al comportamiento habitual de consumo sea previamente validada, a efectos de poder procesarse en el sistema, sino que habilitan al proveedor a adoptar acciones ante su ejecución.

42. En efecto, el artículo 17° del Reglamento señala que el proveedor debe contar con sistemas de monitoreo de operaciones que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual de consumo del usuario; es decir, se acciona a partir de la ejecución de operaciones de tales características. Asimismo, el artículo 22° del Reglamento dispone que la entidad financiera debe implementar mecanismos para la comunicación inmediata al usuario sobre la ejecución de posibles operaciones de fraude, a efectos de proceder con el bloqueo temporal o cancelación definitiva de la tarjeta, en caso sea necesario.

43. Bajo tales consideraciones, a juicio de esta Sala, la primera operación que debió generar una alerta de consumo no debe ser considerada como inválida únicamente por ser ajena al comportamiento habitual de consumo del señor Agurto, por cuanto su ocurrencia es precisamente la que habilita al proveedor a adoptar acciones oportunas a fin de asegurar el patrimonio de su cliente.

Sobre la validez de la operación de S/ 3 500,00 no reconocida

44. En los casos de operaciones con tarjeta de débito no se desconoce la posibilidad de que las mismas puedan ser objeto de usos fraudulentos; sin embargo, este uso se vería limitado en tanto no se tuviera acceso a la clave secreta, cuyo resguardo es responsabilidad exclusiva del tarjetahabiente; por ello, de acreditarse que la operación se realizó con el uso conjunto de estos dos (2) elementos, la transacción debe reputarse como válidamente realizada.

45. Respecto de la primera (1°) operación -que debió generar una alerta en los sistemas del proveedor- es preciso indicar que fue realizada a través de la plataforma de banca móvil del proveedor, siendo que, a fin de ingresar a la misma, era menester el uso conjunto de la tarjeta de débito respectiva y de su clave secreta.

46. En este punto, conviene puntualizar que no es un hecho controvertido que el señor Agurto se haya encontrado afiliado a la banca por internet, toda vez que ello no ha sido negado por el consumidor, siendo que, de los Estados de Movimientos de la Cuenta en Soles 0011-****-****-0834 y la Cuenta en Dólares

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

0011-****-****-3831[5], se ha verificado que, con anterioridad a la ejecución de las operaciones controvertidas, el denunciante realizó otras operaciones a través de ese canal.

47. A efectos de acreditar su falta de responsabilidad, el Banco aseveró, entre otros puntos, lo siguiente:

    (i) La validez de esta operación quedó registrada en el reporte denominado "Log de Operaciones KT80", en donde se apreciaba que, el 5 de agosto de 2021, a las 17:31:19 horas, se registró el ingreso correcto a la Banca GNET (J2A1) con el uso correcto de la clave, registrándose la operación de manera satisfactoria a las 17:31:20 horas[6]; y,
    (ii) dado que las operaciones antes señaladas fueron transferidas entre las propias cuentas del señor Agurto, no se requirió la clave token digital, información que fue consignada en los reportes con el comando BQ46.

48. Al respecto, si bien a consideración del Banco los medios probatorios citados previamente demuestran el ingreso correcto a la Banca por internet y la autorización de las operaciones cuestionadas, lo cierto es que de su lectura esta Sala aprecia que las cuentas bancarias de origen y de destino consignadas no son congruentes con lo expuesto por las partes en el procedimiento (cuentas propias del denunciante); es decir, hacen referencia a cuentas distintas (tanto de origen como destino)[7] a las cuales fueron afectadas, sin que la entidad denunciada haya cumplido con sustentar el motivo de dicha incongruencia.

49. Aunado a lo anterior, aun cuando el denunciado refirió que las operaciones en cuestión eran transferencias (hecho que se colige del medio probatorio aportado por este); de la revisión del Estado de Movimiento de la cuenta del denunciante, se observa que el concepto de la operación fue denominado "SAGAFALABELLA", lo cual tampoco guarda relación con los argumentos de defensa expuestos por la entidad bancaria, quien no ha sustentado la razón de la denominación consignada en dicho documento.

50. De ahí que este Colegiado considera que los medios probatorios presentados por el Banco no generan la suficiente convicción para eximirlo de responsabilidad, máxime si el denunciado se encontraba en mejor posición de acreditar que el hecho denunciado en su contra no le era atribuible.

---

5 Ver de la foja 70 a la 76 del expediente.

6 Ver la foja 66 del expediente.

7 Cabe señalar que el medio probatorio denominado "Log de Operaciones KT80" hace referencia a las Cuentas 0011-****-****-7808 y 0011-****-****-7103, bajo la glosa de SAGAFALABELLA, siendo que las cuentas afectadas objeto de controversia responden a la numeración 0011-****-****-0834 y 0011-****-****-3831.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

51. Por lo expuesto, corresponde revocar la resolución venida en grado, en el extremo que declaró infundada la denuncia interpuesta contra el Banco; y, en consecuencia, declarar fundada la misma, por infracción del artículo 19° del Código, al haberse verificado que no adoptó las medidas de seguridad necesarias en el procesamiento de cuatro (4) operaciones no reconocidas, consistentes en transferencias por el importe total de S/ 31 000,00 desde su cuenta en soles a su cuenta en dólares.

Sobre la graduación de la sanción

52. El 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 (en adelante, el Decreto Supremo), establece que los parámetros contemplados en su contenido deben ser aplicados por, entre otros, la Sala, para los procedimientos iniciados a partir de su entrada en vigencia (a saber, el 14 de junio de 2021).

53. En el caso en concreto, esta Sala ha determinado la responsabilidad del proveedor por la falta de adopción de medidas de seguridad en el procesamiento de cuatro (4) operaciones no reconocidas, por lo que corresponde efectuar un análisis de la graduación correspondiente.

54. Dado que el inicio del procedimiento ocurrió el 23 de setiembre de 2021 (oportunidad en la que la normativa antes señalada ya se encontraba vigente), corresponde a este Colegiado efectuar la graduación de la multa a imponer a la entidad financiera en atención a lo dispuesto en dicho cuerpo normativo.

55. Ahora bien, teniendo en cuenta que la conducta infractora materia de análisis se suscitó por un periodo menor a dos (2) años, no dañó ni puso en riesgo la vida y/o salud de las personas y careció de un alcance geográfico nacional, esta Sala considera que resulta pertinente graduar la sanción a imponer de acuerdo con el “Método basado en valores preestablecidos”, siendo, en particular, aplicable el “Método de valores preestablecidos para otras infracciones en OPS, CPC y SPC”. Así, a efectos de determinar la sanción aplicable, desarrollaremos el análisis que corresponde por la metodología antes citada:

Etapa I: Multa base (m):

(i) Determinada al multiplicar los valores preestablecidos de acuerdo al nivel de afectación de la infracción y el tamaño del infractor (k) por el factor de duración (D), conforme a lo siguiente fórmula: **(m) = (k) * (D)**;

(ii) para determinar el factor del nivel de afectación de la infracción (k), se verifica que la infracción denunciada se encontraba vinculada a “**Infracciones donde la cuantía afectada del bien o servicio**

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

denunciado sea superior a (04) UIT y menor a (08) UIT", en tanto, el valor del objeto materia de reprogramación unilateral era de S/ 31 000,00, importe equivalente aproximadamente a 6,7 UIT;

(iii) en virtud de ello, su nivel de afectación era "moderado", conforme a lo establecido en el Cuadro 16 del Decreto Supremo;

(iv) con respecto al tamaño del proveedor denunciado, en aplicación de los Principios de Legalidad y Uniformidad[8], se logra apreciar los estados financieros publicados por el Banco por el periodo anual de 2021 -año de la ocurrencia de la conducta infractora[9]- que es pertinente atribuir al proveedor la condición de **gran empresa**;

(v) en concordancia con el nivel de afectación de la infracción, en términos de UIT, corresponde considerar como valor de (k) el monto de 11,60 UIT, conforme a lo establecido en el Cuadro 19 del Decreto Supremo;

(vi) en lo referido el factor de duración (D), se determina que la infracción es de naturaleza instantánea, en tanto, la misma se habría concretado en un momento determinado, por lo que, de acuerdo con el Cuadro 23 del Decreto Supremo corresponde asignarle un valor de 1,0;

(vii) por consiguiente, la multa base (m) se concluye en 11,60 UIT, resultado de multiplicar 11,60 UIT (k) por 1,0 (D).

Etapa II: multa preliminar (M):

(i) valor que resultaba de multiplicar la multa base (m) por los factores agravantes o atenuantes (F), conforme a la siguiente fórmula: **(M) = (m) * (F);**

(ii) no obstante, en el presente caso no se evidencia la configuracion de ningun factor agravante o atenunciante, lo que implicó que dicho factor sea igual a la unidad (F=1 o 100%);

(iii) por consiguiente, corresponde imponer al Banco una multa preliminar (M) de 11,60 UIT, resultado de multiplicar 11,60 (m) por 1 (F);

Etapa III: multa final (*M):**

(i) en este último paso se debe analizar si la multa preliminar (M) se encuentra dentro del tope máximo establecido en el marco normativo de cada órgano resolutivo; en ese sentido, considerando que la infracción

---

8 **TEXTO ÚNICO ORDENADO DE LA LEY 27444. LEY DEL PROCEDIMIENTO ADMINISTRATIVO GENERAL, APROBADO POR EL DECRETO 004-2019-JUS. 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 convertidas en la regla general. Toda diferenciación deberá basarse en criterios objetivos debidamente sustentados.

9 Fuente: Patrón de contribuyentes de la Superintendencia Nacional de Aduanas y de la Superintendencia de Administración Tributaria.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

objeto de acreditación por parte de esta instancia tiene la calidad de moderada[10], se establece que la misma no supera tope legal alguno, por lo que la multa final impuesta (*M**) fue de 11,60 UIT.

56. Por lo expuesto, corresponde sancionar al Banco con una multa de 11,60 UIT, por infracción del artículo 19° del Código.

Sobre la medida correctiva

57. El artículo 114° del Código establece que la autoridad administrativa podrá -a pedido de parte o de oficio- adoptar las medidas que tengan por finalidad revertir los efectos que la conducta infractora hubiera ocasionado o evitar que esta se produzca nuevamente en el futuro.

58. En esa línea, el artículo 115° del Código dispone que la finalidad de las medidas correctivas reparadoras es resarcir las consecuencias patrimoniales directas e inmediatas ocasionadas al consumidor por la infracción administrativa a su estado anterior[11]. Asimismo, el artículo 116° de dicho

[10] **LEY 29571. CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR. Artículo 110°.- Sanciones administrativas.** El órgano resolutivo 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 Nº 807, Ley sobre Facultades, Normas y Organización del Indecopi, se rige por lo establecido en dicha norma, salvo disposición distinta del presente Código.

En caso que el proveedor incumpla un acuerdo conciliatorio o cualquier otro acuerdo que de forma indubitable deje constancia de la manifestación de voluntad expresa de las partes de dar por culminada la controversia, o un laudo arbitral, el órgano resolutivo puede sancionar con una multa entre una (1) Unidad Impositiva Tributaria y doscientos (200) Unidades Impositivas Tributarias. Para la graduación se observan los criterios establecidos en el presente Código y supletoriamente, los criterios que establece la Ley Nº 27444, Ley del Procedimiento Administrativo General o la norma que la sustituya o complemente.

Las sanciones administrativas son impuestas sin perjuicio de las medidas correctivas que ordene el órgano resolutivo y de la responsabilidad civil o penal que correspondan.

[11] **LEY 29571. CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR.**
(…)
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.
(…)

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

cuerpo normativo señala que 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[12].

59. En su denuncia, el señor Agurto solicitó como medida correctiva que el Banco cumpliera con extornar la operación controvertida a su cuenta en soles.

60. Ahora bien, en la medida que ha quedado acreditada la responsabilidad del Banco respecto del hecho infractor, consistente en la falta de adopción de medidas de seguridad para el procesamiento de cuatro (4) transferencias no reconocidas desde su cuenta en soles a su cuenta en dólares; este Colegiado considera que corresponde ordenar al Banco, en calidad de medida correctiva reparadora, que, en un plazo no mayor a quince (15) días hábiles contados a partir del día siguiente de la notificación de la presente resolución, cumpla con anular las transferencias materia de denuncia, dejando sin efecto todos los gastos, cobros u otros generados por ello, debiendo devolver a la Cuenta en Soles 0011-****-****-0834 de titularidad del denunciante, el importe total de S/ 31 000,00, correspondientes a las operaciones no reconocidas, más los intereses que se hubiesen generado, desde la fecha de su realización hasta la del cumplimiento del mandato.

61. Asimismo, se precisa que, en un plazo no mayor de cinco (5) días hábiles contados a partir del vencimiento del plazo otorgado, el Banco deberá presentar ante la Comisión los medios probatorios que acrediten el cumplimiento del mandato, bajo apercibimiento de imponerle una multa coercitiva conforme a lo establecido en el artículo 117° del Código[13].

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 (…)

12 **LEY 29571. CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR.**
(…)
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: (…)

13 **LEY 29571. CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR. Artículo 117º.- 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 resolutivo 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.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

62. Finalmente, se informa que, en caso de incumplimiento, el señor Agurto podrá comunicarlo a la Comisión, la cual evaluará la imposición de la multa coercitiva por incumplimiento de medida correctiva conforme a lo establecido en el artículo 40° de la Directiva 001-2021-COD-INDECOPI[14].

Sobre el pago de las costas y los costos del procedimiento

63. De conformidad con lo establecido por el artículo 7º del Decreto Legislativo 807, Ley Sobre Facultades, Normas y Organización del Indecopi, la Comisión y la Sala pueden ordenar al infractor que asuma el pago de las costas y costos del procedimiento en que haya incurrido el denunciante o el Indecopi[15].

64. El rembolso de las costas[16] y los costos[17] en favor de la parte denunciante tiene por objeto devolverle los gastos que se vio obligada a realizar al acudir ante la Administración para denunciar un incumplimiento de la Ley.

---

14 **DIRECTIVA 001-2021-COD-INDECOPI. DIRECTIVA ÚNICA QUE REGULA LOS PROCEDIMIENTOS DE PROTECCIÓN AL CONSUMIDOR PREVISTOS EN EL CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR. 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 resolutivo 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 resolutivo 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 resolutivo 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 resolutivo 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.

15 **DECRETO LEGISLATIVO 807. LEY SOBRE FACULTADES, NORMAS Y ORGANIZACIÓN DEL INDECOPI. Artículo 7º.-** En cualquier procedimiento contencioso seguido ante el Indecopi, la comisión o dirección competente, además de imponer la sanción que corresponda, puede 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 o dirección del Indecopi puede aplicar las multas de acuerdo a los criterios previstos en el artículo 118° del Código de Protección y Defensa del Consumidor. Quien a sabiendas de la falsedad de la imputación o de la ausencia de motivo razonable denuncie a alguna persona natural o jurídica, atribuyéndole una infracción sancionable por cualquier órgano funcional del Indecopi, será sancionado con una multa de hasta cincuenta (50) Unidades Impositivas Tributarias (UIT) mediante resolución debidamente motivada. La sanción administrativa se aplica sin perjuicio de la sanción penal o de la indemnización por daños y perjuicios que corresponda.

16 **CÓDIGO PROCESAL CIVIL. Artículo 410º.- Costas.** Las costas están constituidas por las tasas judiciales, los honorarios de los órganos de auxilio judicial y los demás gastos judiciales realizados en el proceso.

17 **CÓDIGO PROCESAL CIVIL. Artículo 411º.- Costos.** Son costos del proceso el honorario del Abogado de la parte vencedora, más un cinco por ciento destinado al Colegio de Abogados del Distrito Judicial respectivo para su Fondo Mutual y para cubrir los honorarios de los Abogados en los casos de Auxilio Judicial.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

65. Por tanto, dado que se ha verificado que el Banco incurrió en una infracción del artículo 19° del Código, corresponde ordenar al denunciado que, en un plazo no mayor de cinco (5) días hábiles de notificada la presente resolución, cumpla con pagar al señor Agurto las costas del procedimiento por un monto ascendente a S/ 36,00.

66. Sin perjuicio de ello y, de considerarlo pertinente, el señor Agurto podrá solicitar el reembolso de los montos adicionales en que hubiese incurrido para la tramitación del presente procedimiento, para lo cual deberán presentar una solicitud de liquidación de costos.

67. Asimismo, respecto del pago de las costas y los costos del procedimiento ordenado, se informa al Banco que deberá presentar a la Comisión los medios probatorios que acrediten el cumplimiento de dicho mandato, en el plazo máximo de cinco (5) días hábiles, contado a partir del vencimiento del plazo otorgado para tal fin; bajo apercibimiento de imponer una multa coercitiva conforme a lo establecido en el artículo 118°[18] del Código.

68. Finalmente, se informa al señor Agurto que, en caso de incumplimiento, podrá comunicarlo a la Comisión, la cual evaluará la imposición de una multa coercitiva por incumplimiento del pago de las costas y los costos del procedimiento, conforme a lo establecido en el artículo 41°[19] de la Directiva 001-2021-COD-INDECOPI.

---

18 **LEY 29571. CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR. Artículo 118º.- 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 resolutivo 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.

19 **DIRECTIVA 001-2021-COD-INDECOPI. DIRECTIVA ÚNICA QUE REGULA LOS PROCEDIMIENTOS DE PROTECCIÓN AL CONSUMIDOR PREVISTOS EN EL CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR. 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.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

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

69. En tanto esta Sala ha verificado que el Banco incurrió en una infracción del artículo 19° del Código, corresponde disponer su inscripción en el Registro de Infracciones y Sanciones del Indecopi, de conformidad con lo establecido en el artículo 119° del Código[20].

Sobre la remisión de una copia de la resolución a la Superintendencia de Banca, Seguros y AFP

70. Habiéndose verificado la comisión de la conducta infractora imputada contra el Banco y considerando que la Superintendencia de Banca, Seguros y AFP constituye la entidad reguladora y supervisora de las empresas que operan en el sistema financiero nacional, corresponde a la Secretaría Técnica de la Sala Especializada en Protección al Consumidor remitirle periódicamente copia de las resoluciones que imponen sanciones a dichas empresas en virtud de los procedimientos seguidos en su contra, para que adopte los fines que considere pertinentes.

RESUELVE:

PRIMERO: Revocar la Resolución 0318-2022/INDECOPI-CUS del 26 de mayo de 2022, emitida por la Comisión de la Oficina Regional del Indecopi de Cusco, en el extremo que declaró infundada la denuncia interpuesta por el señor José Antonio Agurto Belloso contra Banco BBVA Perú S.A.; y, en consecuencia, declarar fundada la misma, por infracción del artículo 19° de la Ley 29571, Código de Protección y Defensa del Consumidor, al haberse verificado que no adoptó las medidas de seguridad necesarias en el procesamiento de cuatro (4) operaciones no reconocidas, consistentes en transferencias por el importe total de S/ 31 000,00 desde su cuenta en soles a su cuenta en dólares.

SEGUNDO: Sancionar a Banco BBVA Perú S.A. con una multa de 11,60 UIT, por infracción del artículo 19° de la Ley 29571, Código de Protección y Defensa del Consumidor.

TERCERO: Requerir a Banco BBVA Perú S.A. el cumplimiento espontáneo de pago de la multa impuesta, bajo apercibimiento de iniciar el medio coercitivo específicamente aplicable, de acuerdo a lo establecido en el numeral 4 del artículo 205° del Texto Único Ordenado de la Ley 27444, Ley del Procedimiento

[20] **LEY 29571. CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR. 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.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

Administrativo General, aprobado por el Decreto Supremo 004-2019-JUS, precisándose, además, que los actuados serán remitidos a la Sub Gerencia de Ejecución Coactiva para los fines de ley, en caso de incumplimiento.

CUARTO: Ordenar a Banco BBVA Perú S.A., en calidad de medida correctiva reparadora, que, en un plazo no mayor a quince (15) días hábiles contados a partir del día siguiente de la notificación de la presente resolución, cumpla con anular las transferencias materia de denuncia, dejando sin efecto todos los gastos, cobros u otros generados por ello, debiendo devolver a la Cuenta en Soles 0011-****-****-0834 de titularidad del denunciante, el importe total de S/ 31 000,00, correspondientes a las operaciones no reconocidas, más los intereses que se hubiesen generado, desde la fecha de su realización hasta la del cumplimiento del mandato.

Informar a Banco BBVA Perú S.A. que deberá presentar ante la Comisión de la Oficina Regional del Indecopi de Cusco, los medios probatorios que acrediten el cumplimiento de la medida correctiva ordenada, en el plazo máximo de cinco (5) días hábiles, contado a partir del vencimiento del plazo otorgado para tal fin; bajo apercibimiento de imponer una multa coercitiva conforme a lo establecido en el artículo 117° del Código de Protección y Defensa del Consumidor. De otro lado, se informa que en caso de incumplimiento, la parte denunciante podrá comunicarlo al órgano de primera instancia, la cual evaluará la imposición de la multa coercitiva por incumplimiento de medidas correctivas conforme a lo establecido en el artículo 40° de la Directiva 001-2021-COD-INDECOPI.

QUINTO: Ordenar a Banco BBVA Perú S.A. que cumpla con el pago de las costas y los costos del procedimiento a favor del señor José Antonio Agurto Belloso.

Informar a Banco BBVA Perú S.A. que deberá presentar ante la Comisión de la Oficina Regional del Indecopi de Cusco, los medios probatorios que acrediten el cumplimiento del pago de las costas del procedimiento a favor del denunciante en el plazo máximo de cinco (5) días hábiles, contado a partir del vencimiento del plazo otorgado para tal fin, bajo apercibimiento de imponer una multa coercitiva conforme a lo establecido en el artículo 118° de la Ley 29571, Código de Protección y Defensa del Consumidor. De otro lado, se informa que, en caso de incumplimiento, la parte denunciante podrá comunicarlo al órgano de primera instancia, la cual evaluará la imposición de la multa coercitiva por incumplimiento del pago de las costas y los costos del procedimiento conforme a lo establecido en el artículo 41° de la Directiva 001-2021-COD-INDECOPI.

SEXTO: Disponer la inscripción de Banco BBVA Perú S.A. en el Registro de Infracciones y Sanciones del Indecopi.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

SÉPTIMO: Disponer que la Secretaría Técnica de la Sala Especializada en Protección al Consumidor remita a la Superintendencia de Banca, Seguros y AFP, copia de la presente resolución que sanciona a Banco BBVA Perú S.A. para que dicha entidad adopte las medidas que considere pertinentes.

Con la intervención de los señores vocales Hernando Montoya Alberti, Camilo Nicanor Carrillo Gómez, Julio Baltazar Durand Carrión y Oswaldo Del Carmen Hundskopf Exebio.

HERNANDO MONTOYA ALBERTI
Presidente

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe