RESOLUCIÓN FINAL Nº 0124-2024/INDECOPI-CHT

DELEGACIÓN	:	PROTECCIÓN AL CONSUMIDOR
PROCEDENCIA	:	ÓRGANO RESOLUTIVO DE PROCEDIMIENTOS SUMARÍSIMOS DE PROTECCIÓN AL CONSUMIDOR DE LA OFICINA REGIONAL DEL INDECOPI ÁNCASH – SEDE CHIMBOTE
DENUNCIANTE	:	AYELEN MILENA RAMOS CABALLERO
DENUNCIADO	:	BANCO DE CRÉDITO DEL PERÚ S.A.
MATERIA	:	DEBER DE IDONEIDAD
ACTIVIDAD	:	OTROS TIPOS DE INTERMEDIACIÓN MONETARIA

Chimbote, 20 de junio de 2024

I. ANTECEDENTES

1. El 02 de febrero de 2024, la señora Ayelen Milena Ramos Caballero (en adelante, la señora Ramos)1 denunció a Banco de Crédito del Perú S.A. (en adelante el Banco)2; por infracción a la Ley 29571, Código de Protección y Defensa del Consumidor (en adelante, el Código)3.

2. Mediante Resolución N° 01 del 05 de marzo de 2024, el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor de la Oficina Regional del INDECOPI Áncash – Sede Chimbote (en adelante ORPS) 4 decidió iniciar procedimiento administrativo sancionador contra el Banco, de acuerdo al siguiente detalle:

> *"PRIMERO: Iniciar un procedimiento administrativamente sancionador contra Banco de Crédito del Perú S.A., por presunta infracción a lo establecido en el artículo 19 del Código de Protección y Defensa del Consumidor, debido a que, no habría adoptado las medidas de seguridad necesarias para evitar que se realicen el 14 y 15 de diciembre de 2023, tres (3) operaciones por los importes de S/ 4 584,00; S/ 2 000,00; y, S/ 1 914,00 con cargo a su Cuenta de Ahorros N° 310- 19560592605317 de titularidad de la denunciante, los cuales no reconoce, y no pertenece a su comportamiento habitual, conforme el siguiente detalle:*

Fecha	*Detalle*	*Importe*
14/12/2023	*TRAN CTAS TERC*	*S/ 4 584,00*
15/12/2023	*TRAN CTAS TERC*	*S/ 2 000,00*
15/12/2023	*TRAN CTAS TERC*	*S/ 1 914,00"*

3. El 19 de marzo de abril de 2024, el Banco presentó su escrito de descargos, señalando lo siguiente:

(i) la señora Ramos no ha cumplido con acreditar fehacientemente, mediante un medio probatorio pertinente, que su representada hubiera incurrido en la supuesta infracción a las normas de protección al consumidor; y,

1 DNI N° 44248702

2 RUC N° 20100047218

3 LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, publicado el 2 de septiembre de 2010 en el Diario Oficial El Peruano. Dicho código será aplicable a los supuestos de infracción que se configuren a partir del 2 de octubre de 2010, fecha en la cual entró en vigencia el mismo.

4 Ingreso en Comisión Nº 0046-2024-AP/CPC-INDECOPI-CHT

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

(ii) el 04 de enero de 2024, se procedió, por decisión comercial, y en atención al reclamo N° C23376857, a devolver/abonar la suma de S/ 248,96 en la Cuenta de Ahorros N° 310-95805926-0-53 de la señora Ramos Caballero, el cual se logró recuperar de la cuenta beneficiaria de las operaciones cuestionadas, esto es, antes de la interposición de la presente denuncia – 2 de febrero de 2024.

4. Por Resolución N° 02 del 08 de abril de 2024, el ORPS declaró improcedente su prórroga de plazo para presentar la documentación requerida en la resolución de imputación de cargos, de conformidad con lo establecido en el numeral 1 del artículo 9 de la Directiva Nº 001-2021/COD-INDECOPI, Directiva Única que regula los Procedimientos de Protección al Consumidor previstos en el Código.

5. El 10 de abril de 2024, el Banco presentó su escrito complementario de descargos, manifestando lo siguiente:

(i) El 14 de diciembre de 2023, a las 12:25:51 horas y 14:41:26 horas; y a las 17:51:17 horas del 15 de diciembre del mismo año, se registró el ingreso e inicio de la sesión de la señora Ramos en el sistema del aplicativo Banca Móvil BCP; ello, mediante el ingreso del número de su Tarjeta Credimás N° 4557-8804-1491-1374 y su respectiva clave de Internet (06 dígitos);

(ii) es responsabilidad del cliente utilizar en forma adecuada y responsable de la numeración de la tarjeta más la clave de Internet (06 dígitos) del cliente, por ello, toda operación efectuada con la Tarjeta requiere el empleo de la firma electrónica y se reputa indudablemente realizada, reconocida y aceptada por el cliente, y es contabilizada a la fecha en que se realice, aun cuando su empleo fuese realizado por terceros;

(iii) en los casos de extravío o robo de tarjetas, el cliente bajo su exclusiva responsabilidad debe comunicar de inmediato por la vía más rápida posible la pérdida, extravío o destrucción o robo de la tarjeta;

(iv) para realizar operaciones a favor de la cuenta de un tercero (que no haya sido designada previamente como “Favorita”) deberá ingresar su clave Token, las cuales son confidenciales e intransferibles, por lo cual la realización de este tipo de operaciones sin consentimiento del cliente resulta improbable, salvo éste hubiera previamente entregado y/o permitido a terceros el uso de sus claves secretas;

(v) la clave Token se caracteriza por ser un dispositivo electrónico/digital que se encuentra compuesto por seis (06) casilleros de números (del 0 al 9), los cuales cambian de forma aleatoria cada minuto; siendo que, cuando el cliente realiza una operación a favor de la cuenta/servicio de un tercero (que no haya sido designada previamente como “Favorita”) y/o desea guardar/designar una cuenta de destino como “Favorita”, el sistema de la Banca Móvil BCP requiere para su autorización que el cliente haya ingresado los seis (06) números que se encuentren vigentes en el dispositivo Token;

(vi) la denuncia versa sobre tres (03) operaciones no reconocidas por la señora Ramos, las cuales fueron realizadas en dos (02) días (existiendo una diferencia de varias horas entre las operaciones) con cargo a su Cuenta de Ahorros, por lo que no podían ser consideradas como inusuales y/o fraudulentas por sus sistemas antes de su realización, y por ende, no existían indicios que conllevaran a la activación previa de las alertas de seguridad;

(vii) se deberá tener en cuenta pronunciamientos anteriores por parte del Indecopi, como en la Resolución Final N° 952-2014/PS2; N° 1072-2017/CC1; N° 1988-2023/PS2 y, N° 1993-2017/PS2;

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

(viii) realizadas conforme a los estándares de seguridad que establece para todos sus clientes; es decir, fueron realizadas a través del canal de Banca Móvil BCP de nuestra empresa, con el uso correcto y conjunto de la numeración de la Tarjeta Credimás de la señora Ramos y su clave secreta, mientras su tarjeta se encontraba activa; y,

(ix) reiteró sus alegaciones referidas a que se debe tener en cuenta al momento de resolver la devolución parcial de S/ 249,96, de las operaciones no reconocidas, el 04 de enero de 2024.

6. Por Resolución N° 03 del 15 de abril de 2024, el ORPS realizó requerimiento de información al Banco, a fin de analizar el hecho denunciado. Tales requerimientos consistieron en los siguientes:

> *"(...)*
> *(i) Señalar cuáles son los dos (2) factores biométricos o los dos (2) factores de autenticación reforzada de naturaleza distinta e independiente – contemplados en el literal j) del artículo 2 del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por Resolución SBS N° 504-2021 (modificado por la Resolución SBS N° 03797-2023) – utilizados por su representada; debiendo precisar, además, los motivos por los que considera que dichos factores son independientes entre sí y de distinta*
> *(ii) naturaleza. Detallar cuál es el código de autenticación y de uso único generado (mediante métodos criptográficos), a partir de los datos específicos de cada operación materia de denuncia. La notificación a la*
> *(iii) denunciante de los datos de la operación exitosa".*

7. El 22 de abril de 2024, el Banco presentó un escrito brindando respuesta al requerimiento realizado a través de la Resolución N° 03, manifestando lo siguiente:

(i) la autoridad competente para indagar aspectos técnicos relacionados al Reglamento de Ciberseguridad y verificar el cumplimiento de este es la Superintendencia de Banca, Seguros y AFP (SBS), y no el Indecopi; por lo que solicita se sirva dejar sin efecto el presente requerimiento; y,

(ii) cualquier cuestionamiento relacionado a la notificación de las operaciones cuestionadas, no tiene injerencia ni desvirtúa la validez de la realización y el cargo de estas, puesto que fueron efectuadas previamente a cualquier notificación, sumado al hecho que la legislación vigente no establece expresamente que la falta de notificación de una operación conlleve a que su previa autenticación/autorización y cargo sean inválidas.

8. Por Resolución Final N° 0071-2024/PS0-INDECOPI-CHT del 25 de abril de 2024, el ORPS decidió:

> *"PRIMERO: Sancionar a Banco de Crédito del Perú S.A. con multa de 3,78 UIT por haber incurrido en infracción a lo establecido en el artículo 19 del Código de Protección y Defensa del Consumidor, al haberse acreditado que no adoptó medidas de seguridad para evitar que se realicen operaciones fraudulentas de los montos de S/ 2 000,00; y, S/ 1 914,00 con cargo a la Cuenta de Ahorros N° 310-19560592605317 de titularidad de la denunciante, pues no fueron realizadas por su persona y no corresponden a su comportamiento habitual; asimismo, se verificó que la operación de S/ 4 584,00 fue cargada indebidamente, conforme el siguiente detalle:*

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

Fecha	Detalle	Importe
14/12/2023	TRAN CTAS TERC	S/ 4 584,00
15/12/2023	TRAN CTAS TERC	S/ 2 000,00
15/12/2023	TRAN CTAS TERC	S/ 1 914,00

SEGUNDO: Requerir a Banco de Crédito del Perú S.A. el cumplimiento espontáneo de la multa, de conformidad con lo establecido en el numeral 4 del artículo 205 del Texto Único Ordenado de la Ley del Procedimiento Administrativo General, bajo apercibimiento de iniciarse el procedimiento de ejecución coactiva respectivo. El sancionado sólo pagará el 75% de la multa si consiente la presente resolución y procede a cancelarla en un plazo no mayor a quince (15) días hábiles contados a partir del día siguiente de la notificación de la presente Resolución, conforme a lo establecido en el artículo 113 del Código de Protección y Defensa del Consumidor. TERCERO: Ordenar a Banco de Crédito del Perú S.A. como medida correctiva que en un plazo de quince (15) días hábiles, contados a partir del día siguiente de notificada la presente resolución, cumpla con lo siguiente: (i) devolver a la denunciante la suma de los importes S/ 4 584,00; S/ 2 000,00; y, S/ 1 914,00; que corresponde a las tres (3) operaciones indebidas realizadas en su Cuenta de Ahorros N° 310-19560592605317, menos los S/ 249,96 que fueron devueltos previamente en dicha cuenta. Banco de Crédito del Perú S.A. deberá acreditar el cumplimiento de lo dispuesto en el presente artículo, ante este Órgano Resolutivo, en el plazo máximo de cinco (5) días, contados a partir del vencimiento de plazo otorgado en el párrafo precedente, bajo apercibimiento de imponerle una multa coercitiva por incumplimiento de mandato, conforme a lo señalado en el artículo 117 del Código de Protección y Defensa del Consumidor y en los términos y condiciones indicados en la presente resolución. CUARTO: Ordenar a Banco de Crédito del Perú S.A. al pago de las costas del procedimiento y disponer que en un plazo no mayor a quince (15) días hábiles contado a partir del día siguiente de la notificación de la presente resolución, cumpla con el pago de las costas de esta instancia a la denunciante ascendente a S/ 36,00, sin perjuicio del derecho de ésta de solicitar la liquidación de los costos una vez concluida la instancia administrativa. La evaluación de las solicitudes de liquidación estará a cargo del Órgano Resolutivo de Procedimientos Sumarísimos competente. QUINTO: Informar a las partes que la presente resolución tiene vigencia desde el día de su notificación y no agota la vía administrativa. En tal sentido, se informa que de conformidad con lo dispuesto en el numeral 32.1 de la Directiva N° 001-2021/DIR-COD-INDECOPI, contra lo dispuesto por la presente jefatura procede el recurso impugnativo de apelación. Cabe señalar que dicho recurso deberá ser presentado ante el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor de la Oficina Regional del Indecopi Ancash –Sede Chimbote en un plazo máximo de quince (15) días hábiles contados a partir del día siguiente de su notificación, caso contrario la resolución quedará consentida. SEXTO: Informar a las partes que, conforme se dispone en el artículo 34 de la Directiva N° 001-2021/DIR-COD-INDECOPI, las resoluciones de los Órganos Resolutivos de Procedimientos Sumarísimos de Protección al Consumidor que ponen fin al procedimiento no requieren de una declaración de consentimiento expreso.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

SÉPTIMO: Disponer la inscripción de Banco de Crédito del Perú S.A. en el Registro de Infracciones y Sanciones del INDECOPI, una vez que la resolución quede firme en sede administrativa, conforme a lo establecido en el artículo 119 del Código de Protección y Defensa del Consumidor."

9. El 21 de mayo de 2024, el Banco impugnó la Resolución Final N° 0071-2024/PS0-INDECOPI-CHT, manifestando lo siguiente:

(i) a las 12:25:51 horas del 14 diciembre de 2023, a las 14:41:26 horas y a las 17:51:17 horas del 15 de diciembre de 2023 se registró el ingreso e inicio de la sesión de la señora Ramos Caballero en el sistema del aplicativo Banca Móvil BCP de nuestra empresa; ello, mediante el ingreso del número de su Tarjeta Credimás N° 4557-8804-1491-1374 y su respectiva clave de Internet (06 dígitos), tal como se encuentra registrado en el Reporte "Operaciones BM" de nuestro sistema (visado por funcionario responsable) que obra en el expediente; ello, mediante la glosa denominada "Login";

(ii) el Banco nunca solicita la clave secreta a través de correos electrónicos, nunca se comunica con el cliente por teléfono para pedirle su clave secreta y la clave secreta es de exclusivo conocimiento del cliente;

(iii) cuando un cliente desea realizar operaciones a favor de sus propias cuentas, basta con que el cliente hubiera ingresado al aplicativo Banca Móvil BCP y/o Banca por Internet (según sea el caso) mediante el uso de su clave de Internet (06 dígitos), y para realizar operaciones a favor de la cuenta de un tercero (que no haya sido designada previamente como "Favorita") deberá ingresar su clave Token, las cuales son confidenciales e intransferibles, por lo cual la realización de éste tipo de operaciones sin consentimiento del cliente resulta improbable, salvo éste hubiera previamente entregado y/o permitido a terceros el uso de sus claves secretas;

(iv) el mismo 14 y 15 de diciembre de 2023 se efectuaron – durante la vigencia de dichas sesiones de Banca Móvil BCP – con la numeración de la Tarjeta Credimás N° 4557-8804-1491-1374, de titularidad de la señora Ramos Caballero – y cabe resaltar, mientras dicha tarjeta se encontraba activa;

(v) la validez de las operaciones antes indicadas se encuentra debidamente acreditada mediante el Reporte "Operaciones BM" de nuestro sistema (visado por funcionario responsable) que obra en el expediente, el cual registra – además de la fecha, hora y monto de las mismas, así como el ingreso previo de la clave de Internet (06 dígitos) – el uso de la respectiva clave Token de la denunciante; ello, mediante las glosas "Transferencia Cuenta Tercero" y "SofToken";

(vi) la señora Ramos Caballero no ha alegado y/o sostenido haber efectuado el bloqueo de su Tarjeta Credimás antes de la realización de las operaciones cuestionadas;

(vii) toda operación efectuada con la tarjeta (física o de su numeración) y sus respectivas claves secretas o firmas electrónicas, realizadas a través de la Banca Móvil BCP, se reputa ineludiblemente efectuada, reconocida y aceptada por el cliente, y contabilizada en la fecha en que se realice, aun cuando su empleo fuese realizado por terceros. Para el efecto, el cliente asume la obligación de mantener a buen resguardo y bajo su posesión física la tarjeta, o en su defecto la numeración de la misma, así como en total reserva y en secreto la clave de Internet (06 dígitos) y la clave Token, con facultad de modificar dicha clave de Internet directamente y sin intervención del Banco, en las oportunidades y en las veces que lo considere conveniente, sustituyéndola por nuevos códigos o elementos cada vez que presuma que pueda haber

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

trascendido a terceros; debiendo en todo momento mantenerla en calidad de secreto y de su exclusivo conocimiento y uso personal;

(viii) no hay otro modo de ingresar a la Banca Móvil BCP de nuestra empresa, sino es con el uso de la numeración de la tarjeta más la clave de Internet (06 dígitos) del cliente, por lo que es responsabilidad del cliente utilizar en forma adecuada y responsable la misma, así como mantener la(s) clave(s) secretas en tal condición;

(ix) el Banco ha adoptado diversos mecanismos de seguridad a fin de evitar el fraude en las cuentas de nuestros clientes; sin embargo, debemos ser enfáticos en afirmar que, en el presente caso, no se trata de un defecto o defectos en el sistema de seguridad del Banco; puesto que, las operaciones materia de la presente denuncia se realizaron de acuerdo al proceso regular de validación de operaciones efectuadas por el canal de Banca Móvil BCP; es decir, con la numeración de la Tarjeta Credimás y el ingreso previo de la(s) respectiva(s) clave(s) secreta(s) de la denunciante;

(x) las operaciones materia de denuncia se han efectuado en cumplimiento de las normas técnicas impuestas por el Banco, vale decir, tarjeta (numeración), clave de Internet (06 dígitos) y clave Token; tal como se encuentra acreditado con el Reporte "Operaciones BM" y el Reporte "Log Server" de nuestro sistema (visados por funcionario responsable) que obran en el expediente;

(xi) el Reporte "Operaciones BM" de nuestro sistema (visado por funcionario responsable) que obra en el expediente, registran la siguiente información:

(xii) - La fecha y hora de las operaciones, el número de la tarjeta utilizada, el número de la cuenta de origen y de destino; el importe y moneda de las operaciones; el correcto ingreso del número de tarjeta y clave de Internet (06 dígitos), mediante la glosa "Login";

(xiii) El uso de la clave Token para autorizar las operaciones cuestionadas, mediante las glosas "Transferencia Cuenta Tercero" y "SofToken"; asimismo, en el Reporte "Log Server" de su empresa (visado por funcionario responsable), el cual obra en el expediente, se registra la siguiente información: La fecha y hora en que se utilizó la clave Token, Nombre y/o código interno del cliente al que le pertenece la clave Token, el número de serie de la clave Token, el correcto ingreso de la clave Token para autorizar las operaciones cuestionadas, mediante la glosa "Result: Authentication method success", el Banco nunca solicita la clave secreta a través de correos electrónicos, el Banco nunca se comunica con el cliente por teléfono para pedirle su clave secreta, la clave secreta es de exclusivo conocimiento del cliente.

(xiv) de esta manera, se ha podido corroborar y confirmar que dichas operaciones fueron realizadas previo inicio de la sesión de la Banca Móvil BCP, mediante el ingreso del número de la Tarjeta Credimás y de la clave de Internet (06 dígitos) de la señora Ramos Caballero, así como el uso de la clave Token para autorizar/autenticar las operaciones cuestionadas; es decir, ambas contraseñas, las cuales son claves secretas y que únicamente la denunciante debe conocer. Es así que, las operaciones no reconocidas fueron realizadas cumpliendo con las pautas de seguridad que exige nuestra empresa para verificar las transacciones realizadas a través de nuestro canal de Banca Móvil BCP;

(xv) es el cliente quien asume la responsabilidad de todas aquellas transacciones efectuadas con su tarjeta (física o numeración) empleando la clave personal de identificación, toda vez que nuestra entidad no recibió nunca ninguna llamada de parte de la denunciante para proceder al bloqueo previo y las operaciones fueron realizadas correctamente bajo el uso idóneo de la tarjeta – numeración –, digitación previa de la clave Internet (06 dígitos) – para el ingreso a su sesión

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

a la Banca Móvil BCP – y de la clave Token – para autorizar/autenticar las operaciones cuestionadas –; y por ello, el cliente es plenamente responsable de las operaciones efectuadas de manera previa al bloqueo de la tarjeta;

(xvi) consideran necesario hacer de conocimiento de vuestra Comisión que, las medidas de seguridad se encuentran determinadas por los mecanismos establecidos por el Banco para las operaciones a favor de terceros vía nuestra Banca Móvil BCP, los cuales son la digitación previa del número de la Tarjeta Credimás y la respectiva clave de Internet (06 dígitos) para iniciar e ingresar a su sesión, y la clave Token para autorizar/autenticar las operaciones dirigidas a las cuentas/servicios de terceros que no hubieran sido guardadas previamente como "Favoritas";

(xvii) las operaciones materia de denuncia se han efectuado en cumplimiento de las normas técnicas impuestas por el Banco, vale decir, tarjeta (numeración), clave de Internet (06 dígitos) y clave Token – en el caso de las cuentas/servicios de terceros no guardadas previamente como "Favoritas" –, de conocimiento exclusivo de la denunciante; tal como acreditamos con el Reporte "Operaciones BM" y el Reporte "Log Server" de nuestra empresa (visados por funcionario responsable) que adjuntamos al presente;

(xviii) clave Token se caracteriza por ser un dispositivo electrónico/digital que se encuentra compuesto por seis (06) casilleros de números (del 0 al 9), los cuales cambian de forma aleatoria cada minuto; siendo que, cuando el cliente realiza una operación a favor de la cuenta/servicio de un tercero (que no haya sido designada previamente como "Favorita") y/o desea guardar/designar una cuenta de destino como "Favorita", el sistema de la Banca Móvil BCP requiere para su autorización que el cliente haya ingresado los seis (06) números que se encuentren vigentes en el dispositivo Token.

(xix) la presente denuncia versa sobre tres (03) operaciones no reconocidas por la señora Ramos Caballero, las cuales fueron realizadas en dos (02) días (existiendo una diferencia de varias horas entre las operaciones) con cargo a su Cuenta de Ahorros, es evidente que dichas operaciones cuestionadas no podían ser consideradas como inusuales y/o fraudulentas por nuestros sistemas antes de su realización, y por ende, no existían indicios que conllevaran a la activación previa de las alertas de seguridad de Banco de Crédito, tal como ha sido reconocido por el Indecopi en otros procedimientos similares;

(xx) a fin de que sus clientes puedan realizar operaciones a través de nuestra Banca por Internet (www.viabcp.com) y/o Banca Móvil BCP, tal como ocurrió en el presente caso, éstos deberán ingresar e iniciar su sesión en el sistema de dicho canal y/o aplicativo, mediante el ingreso del número de su Tarjeta Credimás y su clave de Internet (06 dígitos), clave que es de conocimiento exclusivo del cliente, en tanto que la misma es memorizada por éste para utilizarla en cualquier momento, e incluso, el cliente tiene la facultad de modificarla/cambiarla directamente y sin intervención del Banco, en las oportunidades y en las veces que considere conveniente. Asimismo, cuando un cliente desea realizar operaciones a favor de la cuenta/servicio de un tercero (que no haya sido designada previamente como "Favorita") y/o desea guardar/designar una cuenta/servicio de destino como "Favorita", también deberá ingresar su clave Token, la cual es confidencial e intransferible, la misma que se caracteriza por ser un dispositivo electrónico/digital que se encuentra compuesto por seis (06) casilleros de números (del 0 al 9), los cuales cambian de forma aleatoria cada minuto;

(xxi) estos dos (02) factores – clave de Internet (06 dígitos) y clave Token – son de distinta naturaleza, mientras que uno es un código que el cliente conoce (clave

de Internet), el otro es un código que el cliente posee (dispositivo clave Token), los cuales son independientes entre sí, puesto que si éste únicamente conoce/posee uno de ellos, no se podrán concretar a través de dichos canales (Banca Móvil y/o Banca por Internet) las operaciones a favor de las cuentas/servicios de terceros no designadas previamente como "Favoritas";

(xxii) en el presente caso el código de autenticación criptográfico es la clave Token del cliente, el cual es un código generado por una semilla criptográfica a base de un algoritmo que impide que pueda ser adivinado o calculado por un tercero, e incluso por el mismo cliente;

(xxiii) por otro lado, vuestra Comisión deberá tener presente que, el hecho que supuestamente Banco de Crédito no hubiera notificado a la señora Ramos Caballero la constancia de las operaciones luego de su realización, no tiene injerencia ni desvirtúa la validez del cargo/débito de dichas operaciones que fueron realizadas previamente de forma válida, esto mediante el uso/ingreso de la numeración de la Tarjeta Credimás y la(s) clave(s) secreta(s) a través de la Banca Móvil BCP, las cuales son de custodia y conocimiento exclusivo de la denunciante, tal como ha sido demostrado fehacientemente por Banco de Crédito a través de los medios probatorios que obran en el expediente;

(xxiv) la falta de notificación de las operaciones cuestionadas, en el supuesto negado de su ocurrencia, únicamente podría ser considerado/calificado como una afectación al deber de información, mas no podría ni debería incidir en la validez de la realización y el cargo de las operaciones cuestionadas, las cuales fueron procesadas correctamente, al haberse efectuado cumpliendo los requisitos de aprobación/autenticación establecidos por las empresas del sistema financiero – como Banco de Crédito – para este tipo de operaciones, y mientras no existieran elementos suficientes que pudieran haber conllevado a que fuera considerada inusual/fraudulenta ni impedida por el sistema de monitoreo antes de su realización, sumado al hecho que la legislación vigente no establece expresamente que la falta de notificación de una operación conlleve a que su previa autenticación y cargo sean inválidas;

(xxv) lo señalado por el ORPS a través de la Resolución Final impugnada es incorrecto, toda vez que, las operaciones cuestionadas – tal como se aprecia de los medios probatorios que obran en el expediente – fueron correctamente procesadas y cargadas/debitadas en la Cuenta de Ahorros de la señora Ramos Caballero; siendo esto así, solicitamos a vuestra Comisión se sirva desestimar lo resuelto por el ORPS;

(xxvi) el ORPS ha sustentado su Resolución Final señalando que Banco de Crédito no cumplió con el Reglamento de Ciberseguridad, resulta pertinente precisar a vuestra Comisión que, la autoridad competente para indagar aspectos técnicos relacionados al Reglamento de Ciberseguridad y verificar el cumplimiento del mismo es la Superintendencia de Banca, Seguros y AFP, en su condición de entidad supervisora de las empresas del sistema financiero (como Banco de Crédito), y no los órganos resolutivos del Indecopi; siendo esto así, es evidente que el sustento de la Resolución Final impugnada resulta incorrecto, en tanto que cualquier análisis y/o supervisión sobre el cumplimiento de dicho Reglamento por parte de nuestra empresa no puede ni debe ser realizado por el Indecopi, en el marco de los procedimientos administrativos bajo su competencia, como el presente;

(xxvii) solicitan se sirva dejar sin efecto la medida correctiva ordenada por no corresponder;

(xxviii) la graduación de la sanción impuesta a través de la Resolución Final, materia del presente recurso, evidencia una falta de proporcionalidad entre la infracción imputada y la sanción impuesta a Banco de Crédito;

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

(xxix) la sanción impuesta a nuestra empresa sería excesiva, al ser equivalente a S/. 19,467.00, pese a que el importe total de las operaciones cuestionadas asciende a S/. 8,498.00; es decir, la multa impuesta supera en S/. 10,969.00 el valor de dichas operaciones cuestionadas, y a su vez, los argumentos esbozados por el ORPS para efectuar la graduación de la presente sanción carecen de una fundamentación clara, precisa y objetiva, y a su vez, vulneran el Principio de Razonabilidad establecido por la legislación vigente. Es evidente entonces que existe una completa falta de proporcionalidad entre la supuesta infracción imputada y la sanción impuesta;

(xxx) los argumentos esbozados por el ORPS se basan en supuestos y fórmulas genéricas que no justifican la razonabilidad de una multa de 3.78 UIT, equivalente a S/. 19,467.00;

(xxxi) no corresponde la condena de pago de costas y costos del presente procedimiento;

(xxxii) no corresponde la inscripción de Banco de Crédito en el registro antes mencionado;

(xxxiii) conforme lo expuesto, solicitan se sirva revocar dichos extremos de la Resolución Final emitida por el ORPS.

10. El 30 de mayo de 2024, a través del Memorándum N° 0121-2024/PS0-INDECOPI-CHT, el ORPS remitió el expediente a la Comisión de la Oficina Regional del Indecopi Ancash – Sede Chimbote (en adelante, La Comisión).

II. ANÁLISIS

Sobre el deber de idoneidad

11. El artículo 18 del Código establece que la idoneidad es la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe5.

12. Por su parte, el artículo 19 del Código establece que los proveedores son responsables por la calidad e idoneidad de los productos y servicios que ofrecen en el mercado6. En aplicación de esta norma, los proveedores tienen el deber de entregar los productos y prestar los servicios al consumidor en las condiciones informadas o previsibles, atendiendo a la naturaleza de estos, la regulación que sobre el particular se haya establecido y, en general, a la información brindada por el proveedor o puesta a disposición.

5 LEY 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR
Artículo 18.- Idoneidad
Se entiende por idoneidad la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe, en función a lo que se le hubiera ofrecido, la publicidad e información transmitida, las condiciones y circunstancias de la transacción, las características y naturaleza del producto o servicio, el precio, entre otros factores, atendiendo a las circunstancias del caso. 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.

6 LEY N° 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR
Artículo 19.- Obligación de los proveedores El proveedor responde por la idoneidad y calidad de los productos y servicios ofrecidos; por la autenticidad de las marcas y leyendas que exhiben sus productos o del signo que respalda al prestador del servicio, por la falta de conformidad entre la publicidad comercial de los productos y servicios y 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 Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

13. Ante la denuncia de un consumidor insatisfecho que pruebe el defecto de un producto o servicio, se presume iuris tantum que el proveedor es responsable por la falta de idoneidad o servicio que pone en circulación en el mercado. Sin embargo, el proveedor podrá demostrar su falta de responsabilidad desvirtuando dicha presunción, es decir, acreditando que empleó la diligencia requerida en el caso concreto (y que actuó cumpliendo con las normas pertinentes) o probando la ruptura del nexo causal por caso fortuito, fuerza mayor, hecho determinante de un tercero o negligencia del propio consumidor afectado.

14. La señora Ramos denunció al Banco no habría adoptado las medidas de seguridad necesarias para evitar que se realicen el 14 y 15 de diciembre de 2023, tres (3) operaciones por los importes de S/ 4 584,00; S/ 2 000,00; y, S/ 1 914,00 con cargo a la Cuenta de Ahorros N° 310-19560592605317 de titularidad de la denunciante, los cuales no reconoce, y no pertenece a su comportamiento habitual, conforme el siguiente detalle:

Fecha	Detalle	Importe
14/12/2023	TRAN CTAS TERC	S/ 4 584,00
15/12/2023	TRAN CTAS TERC	S/ 2 000,00
15/12/2023	TRAN CTAS TERC	S/ 1 914,00

15. El ORPS resolvió declarar fundada la denuncia interpuesta contra el Banco por infracción a lo establecido en el artículo 19 del Código, en tanto a su criterio, no adoptó medidas de seguridad para evitar que se realicen operaciones fraudulentas de los montos de S/ 2 000,00; y, S/ 1 914,00 con cargo a la Cuenta de Ahorros N° 310-19560592605317 de titularidad de la denunciante, pues no fueron realizadas por su persona y no corresponden a su comportamiento habitual; asimismo, consideró que la operación de S/ 4 584,00 fue cargada indebidamente.

16. En su escrito de apelación, el Banco indicó que, sí existieron dos (02) factores de autenticación como son, la clave de Internet (06 dígitos) y clave Token – son de distinta naturaleza, mientras que uno es un código que el cliente conoce (clave de Internet), el otro es un código que el cliente posee (dispositivo clave Token), los cuales son independientes entre sí, puesto que si éste únicamente conoce/posee uno de ellos, no se podrán concretar a través de dichos canales (Banca Móvil y/o Banca por Internet) las operaciones a favor de las cuentas/servicios de terceros no designadas previamente como “Favoritas”.

17. Asimismo, se deberá tener presente que, el hecho que supuestamente Banco de Crédito no hubiera notificado a la señora Ramos Caballero la constancia de las operaciones luego de su realización, no tiene injerencia ni desvirtúa la validez del cargo/débito de las operaciones, en el supuesto negado de su ocurrencia, únicamente podría ser considerado/calificado como una afectación al deber de información, mas no podría ni debería incidir en la validez de la realización y el cargo de las operaciones cuestionadas.

18. En este punto, la Sala estima relevante puntualizar que, de acuerdo con la garantía legal contemplada en el 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,

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

ineludiblemente, el deber de monitoreo y detección de consumos inusuales o sospechosos.

19. Bajo esta línea, 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. En ese sentido, la autoridad administrativa debe evaluar el cumplimiento de dicha garantía legal, incluso aunque el consumidor no hubiera cuestionado su observancia de forma completa o explícita.

20. Teniendo en cuenta este parámetro de análisis de la responsabilidad de la entidad financiera ante la ejecución de operaciones no reconocidas, conviene puntualizar, de manera preliminar, que no es un hecho controvertido que la Cuenta de ahorros N° 310-19560592605317, asociada a la Tarjeta de Débito 4557-****-****-1374, de la señora Ramos estaba activa, en la oportunidad en que se efectuaron las operaciones.

21. Siendo así, a efectos de corroborar el cumplimiento de las medidas de seguridad referidas al monitoreo de operaciones, por parte del denunciado, es oportuno determinar cuál es el comportamiento habitual de consumo del cliente respecto del producto objeto de cuestionamiento. Así, conviene puntualizar que el numeral 5 del artículo 2 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, como por ejemplo 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.

22. Al respecto, de acuerdo con los términos del artículo 17 del referido reglamento[7], se desprende que las empresas del sistema financiero deben adoptar como medidas de seguridad, entre otras, la implementación de sistemas de monitoreo de operaciones, orientados a detectar aquellas operaciones que no corresponden al comportamiento habitual de consumo del usuario[8], en aras de proteger a los usuarios del cargo de transacciones fraudulentas en las cuentas de sus tarjetas de crédito o débito.

23. 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

[7] REGLAMENTO DE TARJETAS DE CRÉDITO Y DÉBITO, APROBADO POR RESOLUCIÓN SBS 6523-2013.
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.
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.

[8] A partir de, entre otros, la revisión de movimientos que permitan generar un patrón de consumo por el uso de cada producto.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

la entidad bancaria o financiera determine a partir del análisis sistemático de la información histórica de cada usuario.

24. Al respecto, de acuerdo con el razonamiento expuesto previamente por la Sala9, 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 correspondientes a las líneas de crédito

25. y/o cuentas objeto de estudio. Así, para determinar si una operación es inusual o no al comportamiento habitual de consumo del cliente debe considerarse si, previamente, se realizaron, con cargo al producto estudiado, operaciones por importes similares a los controvertidos en sede administrativa.

Es pertinente acotar que el referido estudio debe comprender un análisis que considere la totalidad de canales utilizados 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

26. financiero -salvo pacto en contrario- no limita su uso a determinados canales y/o en determinada frecuencia, dado que estos elementos, por sí solos, no puede llevar a determinar que una operación es inusual o sospechosa, siendo que deben ser analizados en conjunto con la información obtenida del historial de consumos del cliente, referida al importe de las operaciones que usualmente realizaba10. En ese sentido, el presunto uso de la tarjeta de débito de la denunciante en una localidad en la que no residía no importa que las operaciones hubiesen sido inusuales.

Con arreglo a lo mencionado, de la revisión de los estados de cuenta de la cuenta de ahorros N° 210-95805926-0-53, se puede apreciar el patrón de consumo de la denunciante desde diciembre 2022 a noviembre 2023, respecto a las operaciones con montos más elevados en cada periodo, conforme se muestra a continuación:

Fecha	Detalle	Monto
Noviembre 2023 (09-11-2023)	TRAN.CEL.BM.	S/ 1 000,00
Noviembre 2023 (09-11-2023)	RETIRO AG 985731	S/ 1 600,00
Octubre 2023 (11-10-2023)	RET. VENTANILLA	S/ 2 000,00
Setiembre 2023 (05-09-2023)	Pago YAPE a 191936	S/ 200,00
Agosto 2023 (25-08-2023)	Pago YAPE a 310767	S/ 1 000,00
Julio 2023 (25-07-2023)		S/ 4 000,00
Junio 2023 (13-06-2023)		S/ 620,00
Mayo 2023 (30-05-2022)		S/ 399,00
Abril 2023 (17-04-2023)		S/ 345,70
Marzo 2023 (01-03-2023)		S/ 3 000,00
Febrero 2023 (18-02-2023)		S/ 400,00

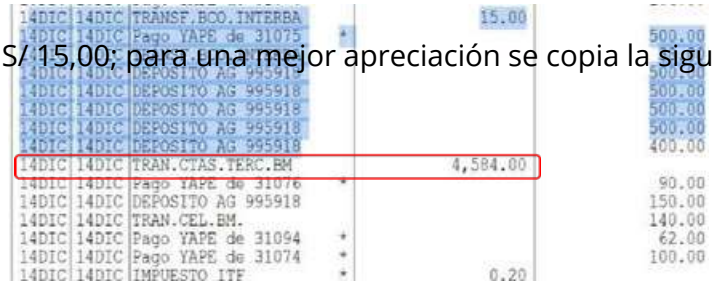
9 Ver Resoluciones 2609-2022/SPC-INDECOPI y 2610-2022/SPC-INDECOPI.

10 A manera de ejemplo, no podríamos 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.

Enero 2023 (20-01-2023)	Pago YAPE a 310044	S/ 240,00
Diciembre 2022 (03-12-2022)	Pago YAPE a 310713	S/ 300,00

27. De la verificación del cuadro reproducido anteriormente, se verifica que la denunciante realizaba consumos frecuentes bajo la modalidad de "yape", y retiro efectivo, cuyo importe más elevado fue de S/ 4 000,00; asimismo, se verifica que realizó operaciones bajo la modalidad de transferencia a terceros "TRAN CTAS TERC"; y, frecuentemente realizaba varias transacciones en el mismo día.

28. De la revisión de los movimientos de la Cuenta de Ahorros N° 310-95805926-0-53,
se verifica que el 14 de diciembre de 2023, la operación de S/ 4 584,00 no fue la primera en efectuarse en el día, sino que le corresponde a una transacción por el importe de S/ 15,00; para una mejor apreciación se copia la siguiente imagen:



14DIC	14DIC	TRANSF.BCO.INTERBA		15.00	
14DIC	14DIC	Pago YAPE de 31075	*		500.00
14DIC	14DIC	DEPOSITO AG 995918			500.00
14DIC	14DIC	DEPOSITO AG 995918			500.00
14DIC	14DIC	DEPOSITO AG 995918			500.00
14DIC	14DIC	DEPOSITO AG 995918			400.00
14DIC	14DIC	TRAN.CTAS.TERC.BM		4,584.00	
14DIC	14DIC	Pago YAPE de 31076	*		90.00
14DIC	14DIC	DEPOSITO AG 995918			150.00
14DIC	14DIC	TRAN.CEL.BM.			140.00
14DIC	14DIC	Pago YAPE de 31094	*		62.00
14DIC	14DIC	Pago YAPE de 31074	*		100.00
14DIC	14DIC	IMPUESTO ITF	*	0.20	

29. En este punto, resulta importante precisar que es posible utilizar la tarjeta de débito y realizar una primera operación en el día, sin que ello constituya una operación inusual. Sostener lo contrario, implicaría restringir la libertad de los consumidores para realizar transacciones en cajeros, comercios, lugares o montos distintos a los efectuados anteriormente conforme con su historial de consumo; por tanto, no correspondía al Banco levantar una alerta por la primera operación del día, por S/ 150,00.

30. Ahora bien, respecto de la operación cuestionada por S/ 4 584,00 es un importe elevado a comparación con las operaciones que realizaba la denunciante en meses previos; siendo el importe más elevado dentro del patrón de consumo de la denunciante, pues, anteriormente, el 25 de julio de 2023, realizó un retiro por un monto alto, de S/ 4 000,00; sin embargo, la transacción cuestionada, resulta superior a la de julio, siendo este un factor que el Banco debió haber advertido como un comportamiento irregular.

31. Este Colegiado considera que la operación por S/ 4 584,00 resultaba ser una operación inusual en el patrón de consumo de la denunciante, ya que después de una transacción de S/ 150,00, realizó una operación muy elevada; además, que supera a las anteriores transacciones efectuadas en meses previos; por lo que, le correspondía levantar una alerta y proceder con la solicitud de confirmación al titular o, en su defecto, realizar el bloqueo preventivo; sin embargo, de la revisión de los medios probatorios presentados que obran en el expediente, no se verifica que el Banco lo haya realizado.

32. En ese sentido, el Banco al no haber adoptado las medidas de seguridad necesarias para proceder con la solicitud de confirmación al titular o con bloqueo preventivo, después de la operación de S/ 4 584,00, al ser considerada sospecha e inusual, las

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

siguientes operaciones de S/ 2 000,00; y, S/ 1 914.00, resultan ser operaciones indebidas.

33. Ahora bien, superado el filtro de monitoreo respecto a la operación de S/ 4 584,00

34. corresponde analizar la validez de su cargo en la cuenta de la denunciante.

35. Al respecto, el 23 de febrero de 202111, la Superintendencia de Banca, Seguros y AFP (en adelante, SBS) publicó el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por Resolución SBS N° 504-2021 (en adelante, Reglamento de Ciberseguridad) que contempla disposiciones legales aplicables para el sistema de gestión de seguridad de la información, que tiene como objetivo principal fortalecer las capacidades de ciberseguridad y procesos de autenticación por parte de las empresas supervisadas por la SBS12 para la realización de operaciones en un entorno seguro y confiable.

Asimismo, si bien el Reglamento de Ciberseguridad entró en vigor el 1 de julio de 202113, algunas disposiciones como el Subcapítulo III del Capítulo II el cual establece mecanismos de enrolamiento y autenticación reforzada para operaciones por canales digitales y la Tercera Disposición Complementaria Final14 referido a reportes de incidentes de ciberseguridad significativos tenían un plazo de

11 https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1277430
RESOLUCIÓN SBS N° 504-2021, REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD , publicada el 19 de febrero de 2021
Artículo 1.- Alcance.
1.1. El presente Reglamento es de aplicación a las empresas señaladas en los artículos 16 y 17 de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas, al igual que las referidas en los párrafos 1.2 y 1.3.
1.2. También es de aplicación al Banco de la Nación, al Banco Agropecuario, a la Corporación Financiera de Desarrollo (COFIDE), al Fondo MIVIVIENDA S.A., y a las Derramas y Cajas de Beneficios bajo control de la Superintendencia, en tanto no se contrapongan con las normativas específicas que regulen el accionar de dichas instituciones.
1.3. Es de aplicación a las empresas corredoras de seguros de acuerdo con lo dispuesto en la Cuarta Disposición Complementaria Final del presente Reglamento.

12 RESOLUCIÓN SBS N° 504-2021, REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD , publicada el 19 de febrero de 2021
Artículo Décimo. – Vigencia
La presente Resolución entra en vigencia el 1 de julio de 2021, fecha en la que se deroga la Circular G 140-2009, con excepción de lo siguiente: a) Los párrafos 25.1 y 25.2 del artículo 25 del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por el Artículo Primero, que entran en vigencia al día siguiente de publicada la presente Resolución, fecha en la cual se deroga el artículo 7A de la Circular G 140-2009. b) El Artículo Segundo de la presente Resolución entra en vigencia a partir de la auditoría correspondiente al ejercicio 2022. c) Los Artículos Séptimo, Octavo y Noveno de la presente Resolución, entran en vigencia al día siguiente de la publicación de la presente Resolución, con excepción de lo indicado en el inciso d. del presente Artículo. d) El requerimiento asociado a la inclusión conjunta de la información sobre la denominación social de la empresa emisora y el nombre comercial que la empresa asigne al producto de tarjeta de crédito y/o débito, señalado en el Artículo Séptimo de la presente Resolución, así como el requerimiento asociado a la inclusión de la dicha información en los dispositivos de soporte al dinero electrónico, señalado en el artículo Octavo de la presente Resolución; entran en vigencia el 1 de enero de 2022. RESOLUCIÓN SBS N° 504-2021, REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

13

14 Y LA CIBERSEGURIDAD, publicada el 19 de febrero de 2021
CAPÍTULO II SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD (SGSI-C)
SUBCAPÍTULO III AUTENTICACIÓN
(...)
En caso de eventos que afecten la continuidad operativa y que tengan como causa probable un incidente de seguridad de la información, es aplicable lo señalado en el artículo 15 del Reglamento para la Gestión de la Continuidad del Negocio, aprobado por la Resolución SBS Nº 877-2020, sobre reporte de eventos de interrupción significativa.
DISPOSICIONES COMPLEMENTARIAS FINALES TERCERA.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

adecuación hasta el 1 de julio de 202215; siendo aplicables a partir de dicha fecha para las empresas supervisadas por la SBS.

36. Siendo así, es preciso destacar que la Sala, en la Resolución 0201-2024/SPCINDECOP16I ha determinado que plataformas tales como banca móvil, banca por internet, billeteras y plataformas digitales de similares características a las señaladas, están dentro de la definición de canal digital brindada por el Reglamento de Ciberseguridad. En consecuencia, dado que las operaciones cuestionadas fueron aprobadas mediante el canal digital "Multired celular", el cual era administrado por el Banco, se corrobora que dicha plataforma era un canal digital regulado por el Reglamento de Ciberseguridad.

37. Habiendo determinado lo mencionado, es importante destacar que el artículo 19 del Reglamento establece que, para la validez de operaciones por un canal digital que impliquen cargos a productos financieros destinados a favor de terceros -como pagos o transferencia de fondos a terceros-, la contratación de un producto, registro de un beneficiario de confianza, modificación de límites y condiciones se requiere que las entidades del sistema financiero adopten las siguientes acciones: a) El uso de, por lo menos, 2 factores de autenticación que correspondan a categorías distintas17 y sean independientes uno del otro; b) La generación de un código de autenticación mediante métodos criptográficos, cuyo uso debe ser por única vez; y, c) La notificación al usuario de los datos de la operación exitosa.

38. Atendiendo a dicha premisa, cabe indicar que el artículo 18 del Reglamento de Ciberseguridad dispone que las entidades del sistema financiero deben adoptar mecanismos de seguridad en el enrolamiento -afiliación- de un usuario a un canal digital, debiendo estos mecanismos estar orientados mínimamente a la verificación de la identidad del usuario que solicita la operación y la generación de las respectivas credenciales del usuario respecto a su afiliación.

39. En el presente caso, la operación cuestionada corresponde a una transferencia a terceros realizada el 15 de diciembre de 2023; por lo que, el Banco no estaba exento de aplicar lo dispuesto en el artículo 20 del Reglamento de Ciberseguridad.

40. Con la finalidad de verificar la autenticación reforzada dispuesta en el Reglamento de Ciberseguridad, se debe verificar en primer lugar la afiliación de la usuaria al canal digital, es así que el Banco presentó su reporte "Rocket PASSPORT", del cual se logra verificar que la señora Ramos se encontraba afiliada a la banca móvil desde las 09:58 horas del día 03 de octubre de 2020; por lo que, se encontraba

15 Ver la información detallada en el Boletín Semanal SBS Informa N° 7 de marzo de 2021, respecto a la Seguridad de la Información y Ciberseguridad, en el enlace siguiente: https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1147?title=Seguridad%20de%20la%20informaci%C3%B3n%20y%20ciberseguridad:%20nuevo%20reglamento%20para%20promover%20un%20entorno%20seguro%20y%20confiab le%20en%20beneficio%20de%20los%20usuarios%20de%20los%20sistemas%20supervisados Resolución aprobada el 24 de enero de 2024. RESOLUCIÓN 0504-2021. REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD. Artículo 2°. – Definiciones. definiciones: (...) j) Factores de autenticación de usuario: Aquellos factores empleados para verificar la identidad de un usuario, que pueden corresponder a las siguientes categorías: - Algo que solo el usuario conoce. - Algo que solo el usuario posee. - Algo que el usuario es, que incluye las características biométricas. (...)

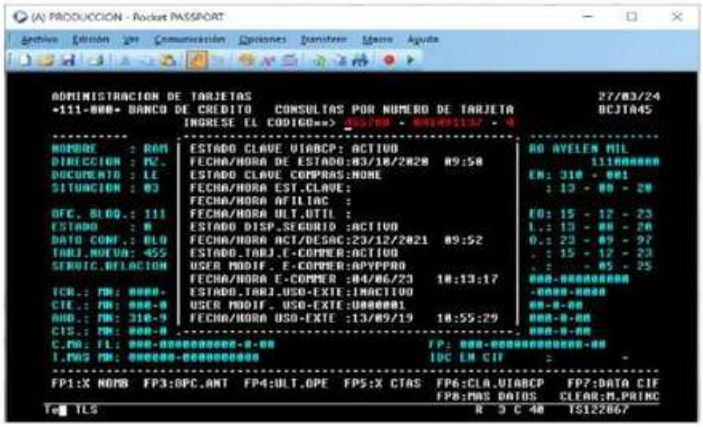
16

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

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

debidamente autorizada para realizar operaciones a través del referido canal. A continuación, se copia el reporte de la afiliación:

REPORTE DE GENERACIÓN DE CLAVE DE INTERNET



41. Posteriormente, se verifica que la denunciante realizó la afiliación a la clave token digital, a las 19:43:08 horas del 12 de noviembre de 2023, con el código serie N° 001921021858:

REPORTE DE AFILIACIÓN A LA CLAVE TOKEN DIGITAL

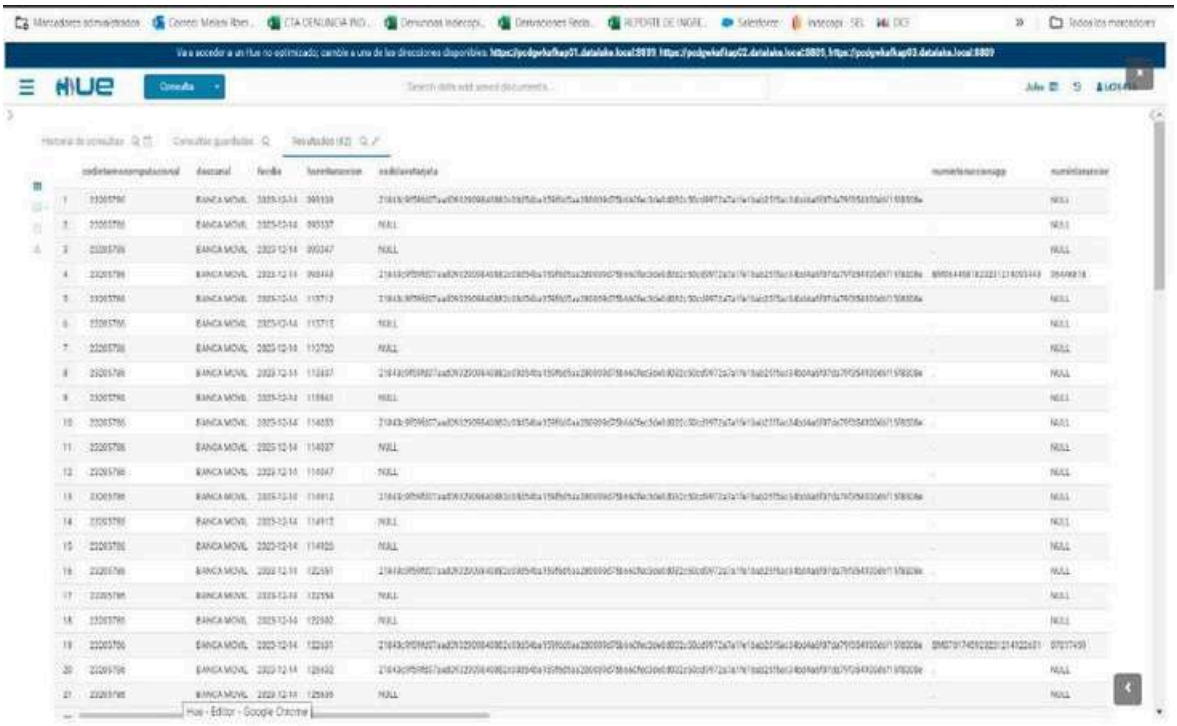
42. En este punto queda acreditado que la señora Ramos se encontraba afiliada a la banca móvil o banca por internet, además de la afiliación de la clave token digital, de manera previa a la realización de las operaciones cuestionadas. Cabe precisar que la denunciante no ha cuestionado su afiliación a la banca móvil o banca por internet en el presente caso.

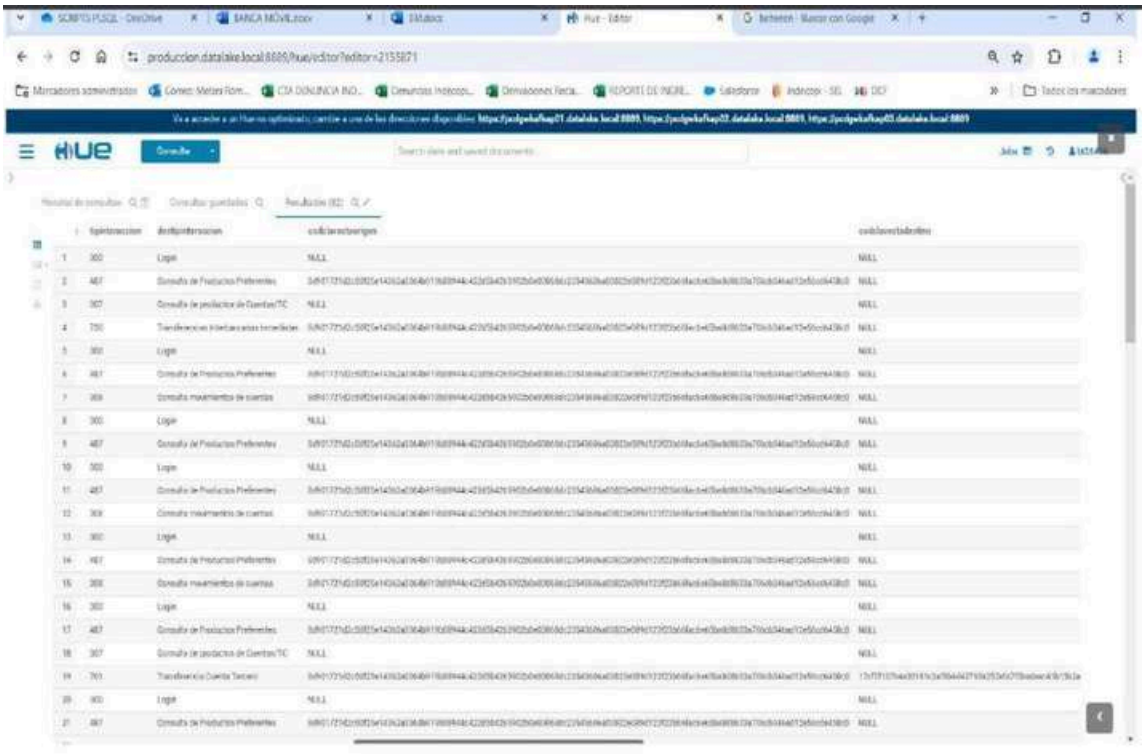
a) La utilización de, por lo menos, 2 factores de autenticación que correspondan a ~~categorías distinta~~s

43. El Banco indicó que en el presente caso se utilizaron dos (02) factores – clave de Internet (06 dígitos) y clave Token – los cuales son de distinta naturaleza, mientras que uno es un código que el cliente conoce (clave de Internet), el otro es un código que el cliente posee (dispositivo clave Token), siendo independientes entre sí, puesto que si éste únicamente conoce/posee uno de ellos, no se podrán concretar a través de dichos canales (Banca Móvil y/o Banca por Internet) las operaciones a favor de las cuentas/servicios de terceros.

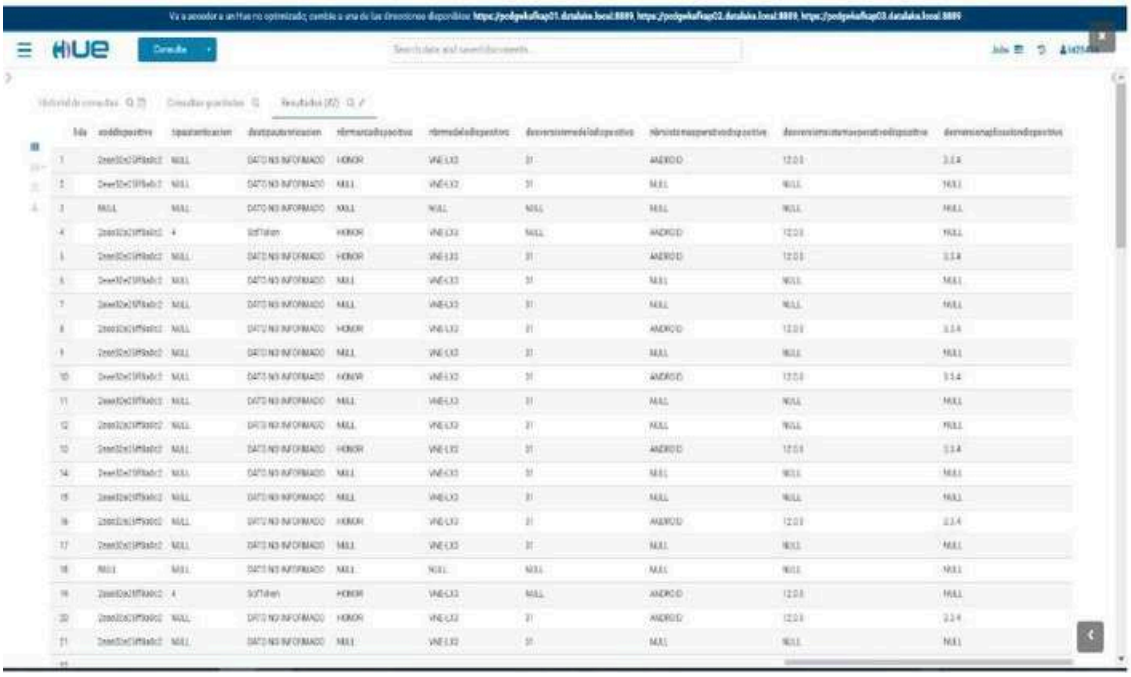
44. Con la finalidad de demostrar dicha utilización, presentó los siguientes reportes, denominados “Log Server”:

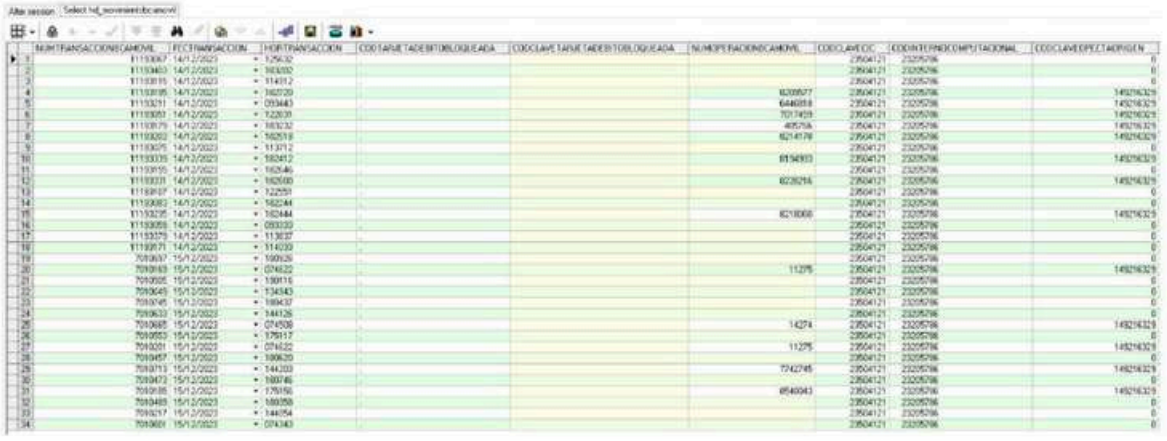
INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

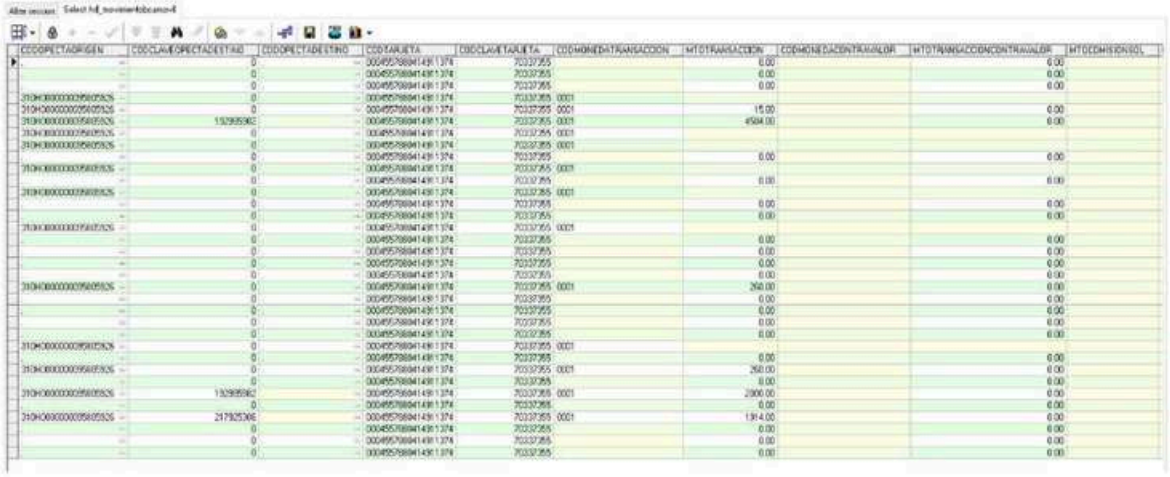




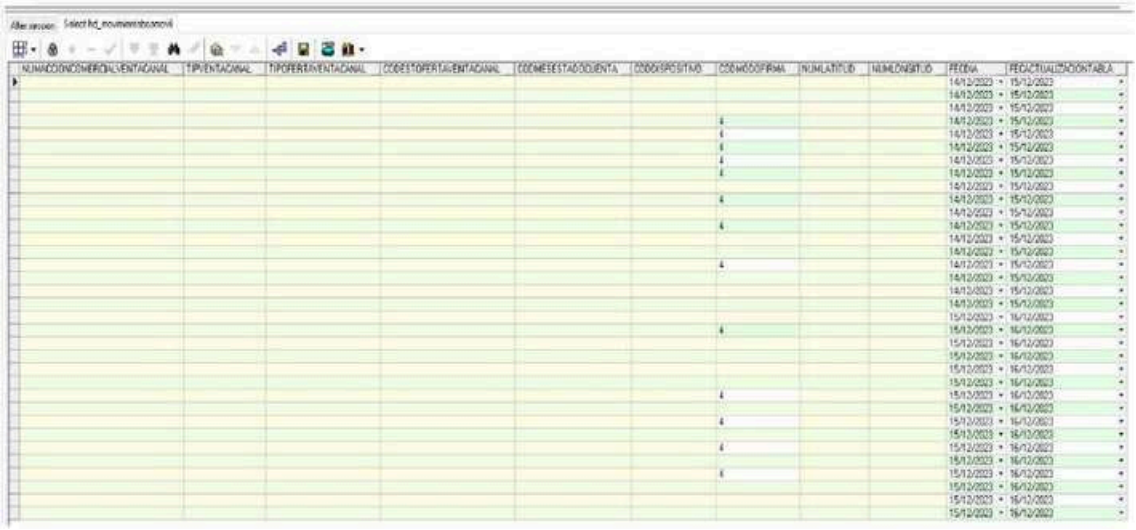
INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe







INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe



45. Esta Comisión considera que, en efecto, de la revisión de los reportes "Log Server" se puede apreciar el ingreso a la aplicación y utilización del "SoftToken" como método de autenticación para la realización de la aplicación; por lo que corresponde valorar el siguiente requisito, consistente en la generación de un código de autenticación mediante métodos criptográficos, cuyo uso debe ser por única vez.

b) ~~La generación de un código de autenticación mediante métodos criptográfi~~cos, cuyo uso debe ser por única vez

46. Con la finalidad de acreditar la utilización del código de autenticación a través de método criptográfico, el Banco presentó su reporte denominado "Log Server", para una mejor apreciación, se copia el mismo:

REPORTE "LOG SERVER"

Date and Time: Fecha y Hora del ingreso del código token
Activity Key: Clave de actividad (Principal Authentication = Autenticación principal)
Action Result Key: Resultado de la clave de acción (Success = Éxito)
Result Key: Resultado de la clave (AUTHN_METHOD-SUCCESS = Método de autenticación exitoso)
Result: Resultado (Authentication method success = Método de autenticación exitoso)
User ID: Código CIC, que es ID del cliente a nivel banco
Token Serial Number: Número de serie token utilizado en la operación

REPORTE CÓDIGO INTERNO COMPUTACIONAL: 23205786

47. Esta Comisión considera que, en efecto, de la revisión del reportes "Log Server" se puede apreciar la utilización exitosa del "SoftToken" como método de autenticación para la realización de la aplicación; por lo que corresponde valorar el siguiente requisito, consistente en la notificación al usuario de los datos de la operación exitosa.

c) La notificación al usuario de los datos de la operación exitosa

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

48. De la revisión del expediente, no se verifica un reporte y/o documento similar que acredite la correcta notificación al usuario conteniendo los datos de la operación exitosa.

49. El Banco indicó que la falta de notificación de las operaciones cuestionadas, únicamente podría ser considerado/calificado como una afectación al deber de información, mas no podría ni debería incidir en la validez de la realización y el cargo de las operaciones cuestionadas, las cuales fueron procesadas correctamente, al haberse efectuado cumpliendo los requisitos de aprobación/autenticación establecidos por las empresas del sistema financiero para este tipo de operaciones.

50. Al respecto, se debe precisar que de acuerdo al Reglamento de Ciberseguridad, se establece que, para tener por válida una operación por un canal digital que impliquen cargos a productos financieros destinados a favor de terceros -como pagos o transferencia de fondos a terceros se requiere que la entidad financiera

51. notifique la validez de la operación con los datos de la misma; situación que no ha sido acreditada, por tanto, no puede considerarse como una operación exitosa el cargo de la operación por S/ 4 584,00 bajo la glosa de transferencia a terceros

En ese sentido, corresponde confirmar modificando fundamentos la resolución venida en grado que declaró fundada la denuncia interpuesta contra el Banco por infracción

Fecha	Detalle	Importe
14/12/2023	TRAN CTAS TERC	S/ 4 584,00
15/12/2023	TRAN CTAS TERC	S/ 2 000,00
15/12/2023	TRAN CTAS TERC	S/ 1 914,00

a lo establecido en el artículo 19 del Código, al haberse acreditado que no adoptó los medidas de seguridad para evitar que se realicen operaciones fraudulentas de montos de S/ 2 000,00; y, S/ 1 914,00 con cargo a la Cuenta de Ahorros N° 310-1936059260059317 de titularidad de la denunciante, pues no fueron realizadas por su persona y no corresponden a su comportamiento habitual, asimismo se verificó que la operación de S/ 4 584,00 fue cargada indebidamente, al no realizarse validación

Graduación de la sanción

52. De conformidad con lo dispuesto en el Decreto Supremo 032-2021-PCM, vigente a partir del 15 de junio de 2021, y aplicable a los procedimientos iniciados a partir de dicha fecha, la multa a imponer por infracciones al Código se calculará en base a la fórmula "M = m x F" donde "m" representa la multa base y "F" la sumatoria de los factores agravantes y atenuantes.

53. Siguiendo el orden previsto en la referida norma, corresponde establecer, en primer lugar, la multa base, para cuyo efecto, se deberá determinar (i) el nivel de afectación en función al tipo de infracción, esto es, si es muy baja, baja, moderada, alta o muy

54. alta; (ii) el tamaño del infractor, verificando, si a la fecha en que cometió la infracción tenía la condición de micro, pequeña, mediana o gran empresa; y, (iii) el periodo de duración de la infracción cometida, que podría ser hasta 24 meses.

De la revisión de la Resolución venida en grado, se verifica que el ORPS consideró los siguientes criterios para establecer el monto correspondiente a la multa:

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre N° 150, Chimbote - Perú / Teléfono: 0800-4-40-40 opción 0 anexo 4901, 012-224777 opción 6 anexo 4901
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

"(i)Nivel de afectación: La infracción cometida está referida a que el Banco permitió que se realicen operaciones fraudulentas de los montos de S/ 2 000,00; y, S/ 1 914,00; asimismo, se verificó que debitó indebidamente el importe de S/ 4 584,00 en la Cuenta de Ahorros N° 310-19560592605317 de la denunciante.

Se determina que el tipo de afectación es "moderada", según el valor preestablecido en el cuadro 16 del Decreto Supremo 032-2021-PCM; toda vez que el importe cuestionado es S/ 8 498,00 (superior a 1 UIT y menor a 2 UIT).

(ii) Tamaño del infractor: El artículo 5 del Texto Único Ordenado de la Ley de Impulso al Desarrollo Productivo y al Crecimiento Empresarial, norma modificada por la Ley 30056, prevé que la condición de micro, pequeña, mediana y gran empresa se obtiene a partir de las ventas anuales (microempresa: ventas anuales de 1 a 150 UIT; pequeña empresa: ventas anuales de 150 a 1 700 UIT; mediana empresa: ventas anuales de 1 700 a 2 300 UIT; y, si las ventas anuales superan las 2 300 UIT se trata de una gran empresa.

De acuerdo con la información económica reportada por el denunciado ante la Superintendencia de Mercados y Valores, en particular, su estado de resultados correspondiente al ejercicio 2022 (año anterior a la fecha de comisión de la infracción), se verifica que sus ventas anuales superaron las 2 300 UIT, considerando para este cálculo la UIT fijada para el 2022 (S/ 4 600,00); por lo que, se ha acreditado su condición de Gran empresa.

Considerando el nivel de afectación y el tamaño del infractor, el valor preestablecido conforme al cuadro 18 previsto en el Decreto Supremo 032-2021-PCM es de 3,78.

(iii) Periodo de duración de la infracción: La infracción se cometió en un solo acto, dada su naturaleza instantánea; por lo que, el factor de duración conforme al valor preestablecido en el cuadro 23 del Decreto Supremo 032-2021-PCM es 1. Al multiplicar el monto preestablecido (3,78) por el factor de duración (1), se determina que la multa base es de 3,78 UIT.

68. Definida la muta base, corresponderá establecer el factor "F", para lo cual se podrán considerar las circunstancias atenuantes y agravantes previstas en el Código, cuyos valores preestablecidos se han recogido en el cuadro 2 del Decreto Supremo 032-2021- PCM. Como las circunstancias atenuantes (AT) solo pueden reducir la multa base hasta en un 50%, es decir, la mitad (el valor en este caso es 0,5); y, las circunstancias agravantes (AG) solo pueden incrementarla hasta en un 100%, es decir, el doble (el valor en este caso es 2,0); el resultado total de sumar los valores asignados a cada circunstancia no podrá exceder dichos topes. En el presente caso, este OPS no verifica la existencia de circunstancias atenuantes ni agravantes.

69. Por tanto, corresponde sancionar el Banco con multa de 3,78 UIT por infracción al artículo 19 del Código."

55. El Banco indicó que el ORPS no ha realizado un análisis adecuado sobre la graduación de las multa impuesta, vulnerando así el principio de razonabilidad; al respecto, es importante precisar que, de la revisión de los factores determinantes usados para la fórmula de la multa, se verifica que están acorde con el Decreto Supremo 032-2021-PCM y se sustentó cada criterio aplicado.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

56. En ese sentido, corresponde confirmar la sanción impuesta al Banco con multa de 3,78 UIT por infracción al artículo 19 del Código. Sobre la medida correctiva, el pago de costos y costas y la inscripción en el Registro de Infracciones y Sanciones

57. En la medida que el Banco no ha fundamento su apelación respecto de los extremos referidos a: (i) la medida correctiva ordenada; (ii) la condena al pago de las costas y costos del procedimiento; y, (iii) su inscripción en el Registro de Infracciones y Sanciones del Indecopi - más allá de la alegada ausencia de responsabilidad desvirtuada precedentemente- se asumen como propias las consideraciones de la recurrida sobre tales puntos.

En ese sentido, se confirma la resolución venida en grado en los extremos que:

58. (i) ordenó al Banco como medida correctiva cumpla con devolver a la denunciante la suma de los importes S/ 4 584,00; S/ 2 000,00; y, S/ 1 914,00; que corresponde a las tres (3) operaciones indebidas realizadas en su Cuenta de Ahorros N° 310-19560592605317, menos los S/ 249,96 que fueron devueltos previamente en dicha

59. cuenta; (ii) condenó al Banco al pago de las costas y costos del procedimiento; y, (iii) dispuso la inscripción del Banco en el Registro de Infracciones y Sanciones del INDECOPI.

Por los fundamentos expuestos y en aplicación de lo establecido en los artículos 105 del Código y 21 literal b) del Decreto Legislativo N° 1033, Decreto Legislativo que aprueba la Ley de Organización y Funciones del Indecopi, la Autoridad Administrativa decide lo siguiente:

III. RESOLUCIÓN:

PRIMERO: Confirmar modificando fundamentos la Resolución Final N° 0071-2024/PS0-INDECOPI-CHT del 25 de abril de 2024, emitida por el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor de la Oficina Regional del Indecopi Ancash – Sede Chimbote, que resolvió sancionar a Banco de Crédito del Perú S.A. con multa de 3,78 UIT18 por haber incurrido en infracción a lo establecido en el artículo 19 del Código de Protección y Defensa del Consumidor, al haberse acreditado que no adoptó medidas de seguridad para evitar que se realicen operaciones fraudulentas de los montos de S/ 2 000,00; y, S/ 1 914,00 con cargo a la Cuenta de Ahorros N° 310- 19560592605317 de titularidad de la denunciante, pues no fueron realizadas por su persona y no corresponden a su comportamiento habitual; asimismo, se verificó que la operación de S/ 4 584,00 fue cargada indebidamente, conforme el siguiente detalle:

Fecha	Detalle	Importe
14/12/2023	TRAN CTAS TERC	S/ 4 584,00
15/12/2023	TRAN CTAS TERC	S/ 2 000,00
15/12/2023	TRAN CTAS TERC	S/ 1 914,00

SEGUNDO: Requerir a Banco de Crédito del Perú S.A. el cumplimiento espontáneo de la multa19, de conformidad con lo establecido en el numeral 4 del artículo 203 del Texto Único

18 Dicha cantidad deberá ser abonada en la Tesorería del Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual - INDECOPI - sito en Calle La Prosa 104, San Borja.

19 Los únicos medios de pago son los siguientes y debe proporcionar para estos efectos el número de CUM para identificar la multa:

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

Ordenado de la Ley del Procedimiento Administrativo General[20], bajo apercibimiento de iniciarse el procedimiento de ejecución coactiva respectivo[21].

TERCERO: Confirmar la Resolución Final N° 0071-2024/PS0-INDECOPI-CHT del 25 de abril de 2024, emitida por el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor de la Oficina Regional del Indecopi Ancash – Sede Chimbote, que ordenó a Banco de Crédito del Perú S.A. como medida correctiva que cumpla con devolver a la denunciante la suma de los importes S/ 4 584,00; S/ 2 000,00; y, S/ 1 914,00; que corresponde a las tres (3) operaciones indebidas realizadas en su Cuenta de Ahorros N° 310-19560592605317, menos los S/ 249,96 que fueron devueltos previamente en dicha cuenta.

CUARTO: Requerir a Banco de Crédito del Perú S.A. que deberá presentar los medios probatorios que acrediten el cumplimiento de la medida correctiva ordenada por el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor de la Oficina Regional del Indecopi Ancash – sede Chimbote, 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 otro lado, se informa a la parte denunciante, que en caso se produzca el incumplimiento del mandato, deberá comunicarlo al Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor de la Oficina Regional del Indecopi Ancash – sede Chimbote, quien evaluará la imposición de la multa coercitiva por incumplimiento de medida correctiva conforme a lo establecido en el numeral 4.11 de la Directiva 006 -2017/DIR-COD-INDECOPI.

QUINTO: Confirmar la Resolución Final N° 0071-2024/PS0-INDECOPI-CHT del 25 de abril de 2024, en el extremo que condenó a Banco de Crédito del Perú S.A. al pago de las costas y los costos del procedimiento.

SEXTO: Confirmar la Resolución Final N° 0071-2024/PS0-INDECOPI-CHT del 25 de abril de 2024, emitida por el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor de la Oficina Regional del Indecopi Ancash – Sede Chimbote, que dispuso la inscripción de Banco de Crédito del Perú S.A. en el Registro de Infracciones y Sanciones

Pago en ventanilla en el Banco de la Nación y Banco de Crédito del Perú	Pago en línea – Internet (solo para clientes de Banco de Crédito del Perú)
1. Indicar que realizará un pago de una multa impuesta por el Indecopi. Cuenta "Indecopi-Multas". 2. Brindar el número de CUM correspondiente. Si paga en Banco de la Nación, deberá indicar el código de transacción 8711 + el número de CUM. 3. Verificar que la constancia del pago indique el número de CUM correcto.	Seguir los siguientes pasos: 1. Seleccionar pagos y transferencias. 2. Seleccionar pago de servicios. 3. Seleccionar Instituciones (Indecopi). 4. Seleccionar el concepto de pago (multas). 5. Ingresar el número de CUM. 6. Ingresar el monto a pagar.

Cualquier abono que no se efectúe en la forma señalada en el cuadro anterior, no será considerado para efectos de la cancelación de la multa. En caso no se cuente con el número de CUM o se presente cualquier inconveniente al pretender efectuar el pago en las modalidades indicadas, será necesario que se comunique inmediatamente a los anexos 7814, 7825 y 7829, así como a la siguiente dirección: controldemultas@indecopi.gob.pe. Sin perjuicio de ello, se le informa que la presente resolución será puesta en conocimiento del Área de Ejecución Coactiva del Indecopi a efectos de que ejerza las funciones que la Ley le otorga.

[20] (footnote marker printed beside the text above)

[21] El procedimiento de ejecución coactiva se encuentra bajo la competencia del Ejecutor Coactivo del Indecopi, y se regula conforma a las normas establecidas en el Texto Único Ordenado de la Ley del procedimiento de ejecución coactiva, aprobado por D.S. N° 018-2008-JUS.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe

del Indecopi, una vez que la resolución quede firme en sede administrativa, conforme a lo establecido en el artículo 11922 del Código de Protección y Defensa del Consumidor.

SÉTIMO: Informar a las partes que la presente resolución tiene vigencia desde el día de su notificación y agota la vía administrativa, por lo que solo puede ser cuestionada en vía de proceso contencioso administrativo ante el Poder Judicial23.

Con la intervención de los señores miembros: Said Giuliano Trujillo Ripamontti, Manuel Ulises Urcia Quispe, Mario Merchán Gordillo y Sadie María Velásquez Contreras.

SAID GIULIANO TRUJILLO RIPAMONTTI
PRESIDENTE

22 LEY Nº 29751, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR Artículo 119º.- 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. LEY Nº 29571. CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR, modificada por el Decreto Legislativo N° 1308. Artículo 125° (...)

23

La Comisión de Protección al Consumidor del Indecopi o la comisión con facultades desconcentradas en esta materia, según corresponda, constituye la segunda instancia administrativa en este procedimiento sumarísimo, que se tramita bajo las reglas establecidas por el presente subcapítulo y por la directiva que para tal efecto debe aprobar y publicar el Consejo Directivo del Indecopi. La resolución que emita la correspondiente Comisión agota la vía administrativa y puede ser cuestionada mediante el proceso contencioso administrativo.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Jr. Elías Aguirre Nº 130, Chimbote – Perú / Teléfonos: 0 800 4 40 40 opción 6 anexo 4301; 01 – 224 7777 opción 6 anexo 4301
E-mail: msanchezq@indecopi.gob.pe / Web: www.indecopi.gob.pe