PONTIFICIA UNIVERSIDAD
CATÓLICA DEL PERÚ

FACULTAD DE DERECHO

Programa de Segunda Especialidad en Derecho Administrativo

La vulneración del principio de confianza legítima en la imputación de la responsabilidad administrativa de las empresas del sistema financiero, por la aplicación del Reglamento Resolución SBS N° 504-2021, en las operaciones no reconocidas con tarjetas de crédito y/o débito

Trabajo académico para optar el título de Segunda Especialidad en Derecho Administrativo

Autor:

Nadia Edith Romero Quispe

Asesor:

*Wendy **Rocio** Ledesma Orbegozo*

Lima, 2024

Informe de Similitud

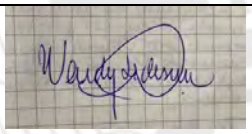
Yo, WENDY ROCIO LEDESMA ORBEGOZO, docente de la Facultad de Derecho de la Pontificia Universidad Católica del Perú, asesor(a) del Trabajo Académico titulado “La vulneración del principio de confianza legítima en la imputación de la responsabilidad administrativa de las empresas del sistema financiero, por la aplicación del Reglamento Resolución SBS N° 504-2021, en las operaciones no reconocidas con tarjetas de crédito y/o débito”, del autor(a) NADIA EDITH ROMERO QUISPE, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 31%. Así lo consigna el reporte de similitud emitido por el software Turnitin el 10/12/2024.

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

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

Lima, 11 de diciembre del 2024

<table>
<tr><td colspan="2">WENDY ROCIO LEDESMA ORBEGOZO</td></tr>
<tr><td>DNI: 10803344</td><td rowspan="2">Firma:  </td></tr>
<tr><td>ORCID: https://orcid.org/0000-0002-5290-8868</td></tr>
</table>

RESUMEN

En un contexto en el que el desarrollo del mercado financiero trabaja en conjunto a las nuevas herramientas de innovación digital, resulta importante un marco regulatorio que pueda brindar las garantías necesarias a favor del consumidor financiero, para que este pueda realizar sus operaciones de forma rápida y eficaz, pero sobre todo con altos niveles de seguridad. Si bien a la fecha, contamos el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, vigente desde el 2022, las posiciones de Indecopi y la SBS se contraponen en relación a su aplicación para efectos de imputar la responsabilidad administrativa de las ESF. Esta situación puede derivar en la vulneración del principio de confianza legítima, y con ello la desconfianza en el mercado tanto para las ESF y los consumidores.

Palabras clave

Operaciones no reconocidas, tarjetas de crédito y débito, canal digital, ciberseguridad, bancos

ABSTRACT

In a context in which the development of the financial market works together with the new digital innovation tools, it is important to have a regulatory framework that can provide the necessary guarantees in favor of the financial consumer, so that he/she can carry out his/her operations quickly and efficiently, but above all with high levels of security. Although to date, we have the Regulation for the Management of Information Security and Cybersecurity, in force since 2022, the positions of Indecopi and the SBS are opposed in relation to its application for the purposes of imputing the administrative responsibility of the ESF. This situation may result in the violation of the principle of legitimate trust, and with it the lack of confidence in the market for both SFEs and consumers.

Keywords

Unrecognized transactions, credit and debit cards, digital channel, cybersecurity, banks

ÍNDICE

I. GLOSARIO DE TÉRMINOS

BCRP	Banco Central de Reserva del Perú
CPDC	Código de Protección y Defensa del Consumidor
ESF	Empresas del Sistema Financiero
Indecopi	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual
Resolución SBS N° 02286-2024	Resolución SBS que modifica el RTCD, el RGCM, el RGSIC y el RRR
RTCD o Reglamento de Tarjetas	Reglamento de Tarjetas de Crédito y Débito, aprobado mediante Resolución SBS N° 6523-2013
RGCM o Reglamento de Conducta	Reglamento de Gestión de Conducta de Mercado del Sistema Financiero, aprobado mediante Resolución SBS N° 3274-2017
RGSIC o Reglamento de Ciberseguridad	Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado mediante Resolución SBS N° 504-2021
RRR o Reglamento de Reclamos	Reglamento de Reclamos y Requerimientos, , aprobado mediante Resolución SBS N°4036-2022
SBS	Superintendencia de Banca, Seguros y AFP
TC	Tribunal Constitucional
TUO de la LPAG	Texto Único Ordenado de la Ley del Procedimiento General, aprobado por Decreto Supremo N° 004-2019-JUS

II. INTRODUCCIÓN

De acuerdo con el BCRP, previo a la pandemia, entre los medios de pagos más utilizados en el mercado financiero se encontraban las tarjetas de débito con un 54%; seguidamente de las transferencias inmediatas con un 39%; y las tarjetas de crédito con un 29%. Con posterioridad a la pandemia, las billeteras digitales se han posicionado con un 93%; seguido de las tarjetas de débito con un 66%; y las transferencias vía banca por internet o banca móvil con un 49%. Cabe indicar además que, las personas han pasado de utilizar solo un instrumento de pago a tres o más instrumentos (2024, p.82).

Esta data nos permite visibilizar que las personas están adoptando entre sus medios de pago a aquellos que les brinden mayores facilidades para realizar operaciones rápidas y eficaces. Situación que excluiría progresivamente al efectivo como medio de pago; debido a factores exógenos como la inseguridad ciudadana, la falsificación de billetes y monedas, entre otros, que han persistido desde larga data.

Ahora bien, específicamente, las tarjetas de crédito y débito, como uno de los medios de pagos más utilizados, se encuentran presentes en nuestras transacciones comerciales diarias. Hoy en día, uno de los mayores usos de tarjetas se realiza a través de su afiliación[1] a las billeteras digitales como yape, plin, agora, entre otros.

Asimismo, las compras que se realizan con las tarjetas, como medio de pago, no solo se realizan a través de canales presenciales; es decir, establecimientos, sino, además, mayoritariamente, mediante canales no presenciales; es decir, a través de comercio electrónico, banca móvil y/o banca por internet. Acorde con ello, el BCRP indicó que, a marzo de 2024, las compras no presenciales con tarjeta de débito y crédito crecieron en 150% y 7%, respectivamente, con respecto a marzo de 2023 (2024:70). Indicadores que evidencian una mayor aceptación y adopción de las compras y/o pagos no presenciales, principalmente

[1] Si bien es cierto que se pueden abrir cuentas con número de Documento Nacional de Identidad, se debe precisar que con ello únicamente se permiten operaciones para el retiro de efectivo en agentes.

por el atractivo de la rapidez con que se realizan aquellas y por el ahorro de tiempo en las largas colas presenciales.

Bajo este contexto, como se desarrollará en el siguiente acápite, los medios de pago distintos al efectivo también han sido objeto de nuevas formas de estafa; y, por ende, han influenciado en diversas modificaciones de regulatorias. En efecto, no es inaudito pensar estas nuevas formas de pago traen consigo una exposición de riesgo para el consumidor financiero mediante canales presenciales y no presenciales. Es por ello que, a través de diversos dispositivos normativos regulatorios, se han ido estableciendo nuevas obligaciones para las ESF, en relación a la implementación de estándares de ciberseguridad y procesos de autenticación más garantistas para la prestación de sus servicios a favor de los consumidores financieros; los límites de responsabilidad administrativa para las ESF en relación a las operaciones no reconocidas con tarjetas de crédito y/o débito; las prácticas adecuadas que adopten las ESF en relación a las operaciones con estos medios de pagos en canales presenciales y no presenciales; entre otros

Estas medidas resultan importantes sobre todo en una relación de consumo, en la que existe una asimetría informativa y además las ESF se encuentran en una mejor posición para afrontar, evitar y contrarrestar aquellos riesgos a los que se encuentran expuestos los consumidores financieros por el uso de sus productos. Además, estas medidas resultan un pilar fundamental para continuar incentivando el uso de diversos medios de pago a través de canales no presenciales y, por ende, la promoción de las iniciativas de interoperabilidad de los sistemas de pagos. La regulación de estos espacios operativos se justifica válidamente en un contexto en donde el desarrollo del mercado financiero trabaja en conjunto a las nuevas herramientas de innovación digital y, por ende, existe un impacto directo en los consumidores financieros.

Es en ese sentido que, una de las últimas modificaciones regulatorias se realizó, el 26 de junio de 2024, a través de la aprobación de la Resolución SBS N° 02286-2024, la cual modifica el Reglamento de Tarjetas, el Reglamento de Ciberseguridad, el Reglamento de Conducta y el Reglamento de Reclamos. Al respecto, específicamente, sobresaltó la modificación del RTCD, al incluir que las ESF asumirían las pérdidas económicas derivadas de las operaciones no

reconocidas, en situaciones donde estas se hubieran realizado sin el empleo de un segundo factor de autenticación. Ahora bien, los métodos de autenticación reforzadas no eran medidas novedad, sino que ya se encontraban reguladas en el RGSIC, la cual resulta aplicable a todos los productos financieros. En esta medida, causa extrañeza la necesidad regulatoria de incluir esta medida en el RTCD, cuando a partir de una interpretación sistemática, las ESF se encontraban obligadas a cumplir con la implementación de los métodos de autenticación reforzada en la utilización de sus productos financieros, desde antes de esta modificación del RTCD.

Esta medida, inicialmente, parecería ser una respuesta a lo que ocurre en la praxis, en la que la aplicación del RGSIC no ha sido necesariamente considerada en todos los tipos de operaciones con tarjetas presentes y no presentes; y, por ende, tampoco a efectos de imputar la responsabilidad administrativa de las ESF. En efecto, como se desarrollará posteriormente, para efectos de imputar la responsabilidad de las ESF, Indecopi realiza el análisis de esta basada en el tipo de canal digital mediante el cual se ha llevado a cabo la operación: banca móvil y/o banca por internet, comercio electrónico, centros comerciales.

En efecto, lo que se buscaría con ello es la protección del consumidor ante la ocurrencia de riesgos por el uso de las tarjetas de crédito y/o débito. Ello se confirma con lo indicado en el Informe de Transferencia de Gestión de Empresa del Estado, emitido en julio de 2024, mediante el cual se desprende que la SBS ha aprobado la Resolución SBS N° 02286-2024, a efectos de complementar las medidas establecidas en el Reglamento de Tarjetas y el Reglamento de Ciberseguridad, cumplir con el Objetivo N° 3 relacionado a “Cautelar que las empresas supervisadas implementen adecuadas prácticas comerciales respetando los intereses y los derechos de los consumidores”, y “seguir fortaleciendo las medidas de prevención ante fraudes en canales digitales” (2024, p. 22).

Ahora bien, atendiendo al contexto y la problemática, en los siguientes acápites se desarrollará la posición de Indecopi sobre la aplicación del RGSIC en relación a las operaciones no reconocidas con tarjetas de crédito y/o débito en diversos canales digitales, a efectos de imputar la responsabilidad administrativa de las ESF. Asimismo, se desarrollará la posición de la SBS respecto a la aplicación

del RGSIC, y cómo a raíz de ello se ha considerado necesaria la regulación de nuevas obligaciones para las ESF a partir de la Resolución SBS N° 02286-2024. Es así como, a partir del análisis de ambas posiciones, se intentará concluir que la vulneración de principio de predictibilidad de las resoluciones administrativas.

Para el desarrollo de lo comentado, (I) se analizará la exposición al riesgo del consumidor financiero por el uso de las tarjetas de crédito y débito en canales presenciales y no presenciales. En esa misma línea, (II) se analizará la regulación normativa sobre las medidas de seguridad en las tarjetas de crédito y débito en los canales digitales. (III) Seguidamente, se determinará la posición de Indecopi, a través del análisis de las resoluciones administrativas, y de la SBS sobre la responsabilidad administrativa de las ESF por las operaciones no reconocidas a través de las tarjetas de crédito y/o débito por compras en canales digitales. Para, finalmente, (IV) analizar la posible vulneración del principio de confianza legítima por las posiciones contrarias en relación a la aplicación del RGISC por las operaciones con tarjeta de crédito y/o débito realizadas a través de comercio electrónico.

Finalmente, para el desarrollo de este análisis se han utilizado instrumentos como la legislación peruana, jurisprudencia y doctrina nacional e internacional en aras de identificar los intereses y derechos constitucionales relevantes tanto para los consumidores financieros como para las ESF.

III. ANÁLISIS DEL AUMENTO DE RECLAMOS Y DENUNCIAS POR OPERACIONES NO RECONOCIDAS POR EL USO DE LAS TARJETAS DE CRÉDITO Y DÉBITO

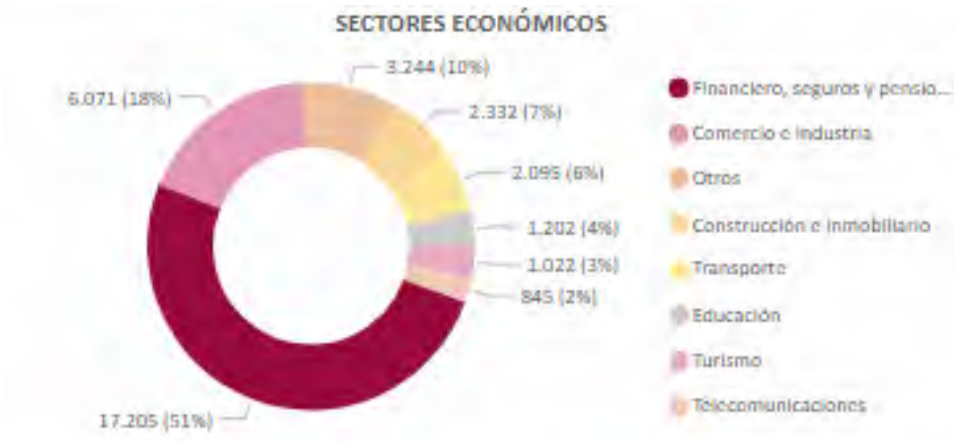
Las tarjetas de crédito y débito son parte de los instrumentos de pago más utilizados por los peruanos para adquirir bienes y/o servicios tanto en canales presenciales y, actualmente mucho más, en canales no presenciales. Como bien es sabido, las tarjetas, como tal, pueden ser representaciones físicas, electrónicas o digitales, de los depósitos y/o créditos con los que cuenta el consumidor financiero en una ESF. En efecto, de acuerdo con los artículos 4 y 5 del RTCD, las tarjetas de crédito, “[...] están asociadas a una línea de crédito, otorgada por la empresa emisora”; mientras que, en la tarjeta de débito, se

realizan las transacciones “[...] con cargo a depósitos previamente constituidos en la empresa emisora”.

Es así como, la facilidad y rapidez con la que se adquieren productos y/o servicios mediante aquel método de pago, ha generado su mayor adopción por parte del consumidor promedio. Al respecto, de acuerdo con Visa Consulting & Analytics, Perú se ha posicionado como uno de los países que realiza más transacciones en línea con tarjetas de débito, lo cual ha mostrado un incremento del 50% en el 2023; así como se cuentan con 8 millones de tarjetas de crédito y casi 44 millones de tarjetas de débito (2023, p. s/n). El aumento del uso de este método de pago, a su vez, implica una alta responsabilidad para las ESF e impacto en el consumidor financiero, ya sea por la disposición de sus propios ahorros o por su calificación crediticia frente a las ESF. Este impacto por el uso de las tarjetas se puede ver afectada, a su vez, ante la falta de medidas de seguridad adecuadas para registrar y validar las operaciones que se realicen a través de aquellas, lo cual desincentivaría su uso.

Al respecto, de acuerdo con Indecopi, de enero a diciembre de 2023, se interpusieron 17 205 denuncias en el sector financiero, seguros y pensiones, con un porcentaje de representación del 51% del total. Ahora bien, específicamente, de las denuncias interpuestas, 6 453 son por tarjetas de crédito y 3 517 por cuentas de ahorros. Es decir, aproximadamente más de la mitad de las denuncias interpuestas por los consumidores financieros son relativas a problemas con estos productos financieros.

Figura 1



Nota: Fuente Indecopi, 2023. A través de esta figura se visualiza que el sector financiero tiene el mayor porcentaje de denuncias en el 2023.

En esa misma línea, de acuerdo con los reportes enviados por las principales ESF a la SBS en el 2024, mediante los cuales indican la absolución de los reclamos por operaciones no reconocidas en las tarjetas de crédito y en las cuentas de ahorro (con y sin tarjeta de crédito), se evidencia la siguiente data desde enero a octubre:

Figura 2

	BBVA		BCP		Interbank	
Absolución a favor	Banco	Usuario	Banco	Usuario	Banco	Usuario
Tarjeta de crédito	6120	7159	2052	6713	13060	26195
Cuenta de ahorro	13385	14099	67604	81481	25072	18213

Nota: Fuente, Elaboración propia en base a los Reportes SBS de enero a octubre de 2024 enviadas por BBVA, BCP e Interbank. A través de esta figura se visualiza la absolución de reclamos por los dos productos financieros.

A partir del gráfico mostrado, se desprende que aproximadamente 61 299 y 219 857 reclamos fueron interpuestos por operaciones no reconocidas en tarjetas de crédito y cuentas de ahorro (con y sin tarjeta de crédito), respectivamente. Asimismo, aproximadamente 127 293 reclamos fueron absueltos a favor de los bancos; es decir, no se realizó devolución alguna a los consumidores financieros por compras que alegaron no haber realizado mediante aquellos productos financieros.

Esta data, nos permite concluir tres aspectos importantes: (I) en los próximos meses podría haber un aumento significativo de denuncias ante Indecopi contra las ESF, respecto al 2023, por operaciones no reconocidas con mayor ahínco en el producto de cuenta de ahorro, seguidamente del producto de tarjeta de crédito; (II) aparentemente habría un mayor índice de incumplimiento de las ESF sobre sus obligaciones relacionadas a las medidas de seguridad; y (III) el aumento de reclamos es paralelo al aumento en el uso de las tarjetas de crédito y/o débito mediante compras en canales presenciales y no presenciales

Sobre este último aspecto, de acuerdo con el reporte estadístico de la Asociación de Bancos del Perú, a setiembre de 2024, los medios de pago no presenciales han tenido un incremento importante, siendo los canales virtuales y banca móvil con un porcentaje de 85.2% y 75.8% de mayor uso; seguidamente de los canales presenciales con un 14.5% de representación (2024, s/n).

En razón de lo expuesto, y sin perjuicio de lo que se desarrollará en el siguiente apartado sobre las medidas de seguridad, se debe indicar que en 2021, la SBS aprobó el RGSIC que entró en vigencia en julio de 2022, el cual resulta exigible a todas las ESF que realicen sus operaciones a través de canales digitales, entre los cuales, como indica, se encuentran principalmente "los aplicativos móviles, páginas web para realizar operaciones (como la banca por internet), las billeteras digitales, los cajeros automáticos (ATM) y los terminales de punto de venta (POS)" (2022, p. s/n).

Por lo tanto, desde el 2022, las ESF se encuentran obligadas a implementar medidas de seguridad en relación a los factores de autenticación para emitir alertas a los usuarios por una operación por encima del patrón de consumo, o validar las operaciones realizadas con tarjetas de crédito y/o débito, no solamente en banca por internet y/o banca móvil, sino en distintos canales digitales donde se realicen estas operaciones.

IV. ANÁLISIS DE LA REGULACIÓN SOBRE LAS MEDIDAS DE SEGURIDAD EN LAS TARJETAS DE CRÉDITO Y DÉBITO EN CANALES DIGITALES

En este apartado, resulta importante poder determinar qué obligaciones tienen las ESF respecto a las operaciones que realizan los usuarios con las tarjetas de crédito y/o débito, ya sea en canales presenciales como, por ejemplo, tiendas físicas, o en canales no presenciales como, por ejemplo, comercio electrónico, banca por internet y/o banca móvil.

Ahora bien, se debe tener presente que, en las resoluciones administrativas de Indecopi, para imputar la responsabilidad de las ESF por operaciones no reconocidas con tarjetas de crédito y/o débito, se analizan dos aspectos importantes, que, desde mi punto de vista, podríamos denominar medidas de alerta y medidas operativas. Las primeras dirigidas a analizar si las ESF,

teniendo en cuenta el patrón de consumo, han podido emitir alertas hacia el usuario, a efectos realizar bloqueos de las tarjetas, para evitar que la transacción se lleve a cabo o, en todo caso, evitar que se continúen realizando posteriores operaciones que no hayan sido autorizadas por el titular. Las segundas dirigidas a verificar, teniendo en cuenta el sistema de autenticación reforzada, si efectivamente la operación realizada ha sido válida.

Cabe indicar que, si bien es cierto que los pronunciamientos de Indecopi al respecto han variado recientemente, como se analizará más adelante, la línea argumentativa de las resoluciones administrativas ha sido aquella. Por lo tanto, a efectos de poder identificar con mayor comprensión la línea argumentativa de la responsabilidad de las ESF, resulta necesario que en este apartado se desarrollen las obligaciones a las que se encuentren sujetas, de acuerdo a las regulaciones vigentes sobre la materia.

IV.1. Reglamento de Tarjetas de Crédito y Débito, aprobado mediante la Resolución SBS N° 6523-2013

Atendiendo a lo mencionado previamente, se procederá a identificar las obligaciones de las ESF en relación con las medidas de ex ante y ex post en las operaciones con las tarjetas de crédito y/o débito.

Respecto a las medidas de alerta, las ESF tienen la obligación de implementar una serie de medidas de seguridad respecto a las operaciones con tarjeta de crédito y/o débito que, de acuerdo con el artículo 17 del RTCD, serán las siguientes: (I) contar con un sistema operativo de monitoreo para detectar las operaciones que no se correspondan con el comportamiento habitual de consumo del usuario; (II) implementar procedimientos para gestionar las alertas generadas por el sistema de monitoreo; por ejemplo, como lo pueden ser las notificaciones al usuario por la operación inusual; (III) identificar patrones de fraude; y (IV) establecer límites y controles en los diversos canales de atención para mitigar las pérdidas por fraude. En esa misma línea, las ESF deberán notificar las operaciones realizadas, que de acuerdo con el artículo 16 numeral 4 del RTCD, deberán ser de forma inmediata después de ser registrada. Los mecanismos para notificar pueden ser los siguientes: mensajes de texto, correo electrónico, llamadas, entre otros, que pueden ser pactados con los titulares.

Cabe indicar que, estas medidas adoptadas por la ESF pueden derivar en dos situaciones: la primera es que el titular cuente con la información de sus transacciones y no realice ninguna acción al respecto, al reconocer que han sido realizadas por el mismo. La segunda es que ante una operación que no haya sido realizada por el titular, este pueda realizar el procedimiento para el bloqueo de su tarjeta y así evitar posteriores operaciones que no reconoce.

Respecto a las medidas operativas, a partir de la publicación de la Resolución SBS N° 2286-2024, también se ha introducido como parte de las medidas de seguridad mínimas que debe adoptar las ESF, el proceso de autenticación del usuario para efectuar operaciones con tarjetas, según corresponda. Es así como, para operaciones con tarjeta presente; es decir, de acuerdo con la definición del RTCD, aquellas operaciones en las que el instrumento de pago interactúa con el dispositivo de captura de información como, por ejemplo, las compras en supermercados, *minimarket*, tiendas por departamento, entre otros, donde cuenten con un procesador de tarjetas, se requerirán dos factores de autenticación: el primero será el chip de la tarjeta o su representación digital; y el segundo, será una clave secreta (PIN) u otro que determine la SBS.

Mientas que, para las operaciones con tarjeta no presente; es decir, de acuerdo con el RTCD, aquellas operaciones en las que el instrumento de pago no interactúa con el dispositivo de captura de información como, por ejemplo, las compras o pagos por comercio electrónico, banca por internet y/o banca móvil, se requerirán dos factores de autenticación. El primero son los datos contenidos en la representación física o digital de la tarjeta; y el segundo, un código dinámico de la tarjeta u otro factor verificable en línea requerido al usuario. Asimismo, en el caso de operaciones con billetera móviles de terceros basadas en *tokenización* de tarjetas; por ejemplo, las operaciones que se realizan por *google pay* y/o *apple pay*, el primer factor de autenticación es la *tokenización* de la tarjeta; y el segundo, otro factor de distinta naturaleza.

Respecto a estas medidas, resulta importante indicar que antes de la modificación del RTCD, en la que se incorporada medidas de seguridad en las operaciones de tarjetas de crédito y débito indicadas en el Reglamento de Ciberseguridad, las ESF ya se encontraban obligadas a adoptar estas medidas, mas en la praxis, como se desarrollará más adelante, se entendía que la

aplicación del Reglamento de Ciberseguridad solo se restringía a las operaciones con tarjeta de crédito y/o débito que se realizaran en banca móvil y/o banca por internet, mas no en los comercios electrónicos. Situación que, además, limitaba la responsabilidad de las ESF en las operaciones no reconocidas.

En esa misma línea, el RTCD indica claramente que, por las operaciones realizadas incorrectamente, la ESF es responsable de realizar la evaluación correspondiente y de demostrar que las operaciones fueron autenticadas y registradas. Es decir, las ESF tienen la carga de la prueba de demostrar que realizaron válidamente la operación, lo cual resulta adecuado sobre todo si atendemos al principio anglosajón *the cheapest cost avoider.* Este, de acuerdo con Espinoza, es un enfoque legal y económico desarrollado por el destacado jurista Guido Calabresi que busca asignar la responsabilidad a la parte que está en la mejor posición para evitar los costos del daño (2019, pp.308-310). En efecto, atendiendo a que las ESF deben implementar medidas de seguridad para evitar que la transacción no reconocida se lleve a cabo, justamente es la que se encuentra en mejor posición, desde el punto de vista operativo, para evitar los costos del daño.

Ante este panorama, mediante el artículo 23 del RTCD, se ha establecido taxativamente bajo qué supuestos las ESF son responsables por las pérdidas de las operaciones realizadas. Estas son las siguientes: (I) incumplimiento de los mecanismos de comunicación a disposición de los usuarios; (II) clonación de tarjetas; (III) por funcionamiento defectuoso de los canales o sistemas en donde se realizan las operaciones; (IV) por manipulación de los cajeros automáticos; (V) suplantación del usuario; (VI) micropagos; (VII) operaciones realizadas luego del bloqueo o cancelación de la tarjeta de crédito y/o débito; (VIII) operaciones no solicitadas o habilitadas por el titular; (IX) el esquema de autenticación del cliente no cumpla con los requerimientos mínimos de seguridad; (X) operaciones realizadas sin el segundo factor de autenticación, donde no se hayan establecidos reglas de aceptación o rechazo, de acuerdo al sistema de monitoreo de transacciones descrito en el artículo 17 del RTCD.

Cabe indicar además que, además la ESF es responsable de las operaciones realizadas con posterioridad a la comunicación efectuada por el usuario sobre el

extravío, robo o uso no autorizado de la tarjeta, o de la información que contiene. Sin perjuicio de ello, el RTCD brinda una pequeña apertura para indicar que la ESF no sería responsable a asumir las pérdidas por las operaciones no reconocidas cuando acredite la responsabilidad del usuario. No obstante, incluso ante ello, se señala que en los casos de micropagos, el solo uso de la tarjeta o de su información no acredita la responsabilidad del usuario.

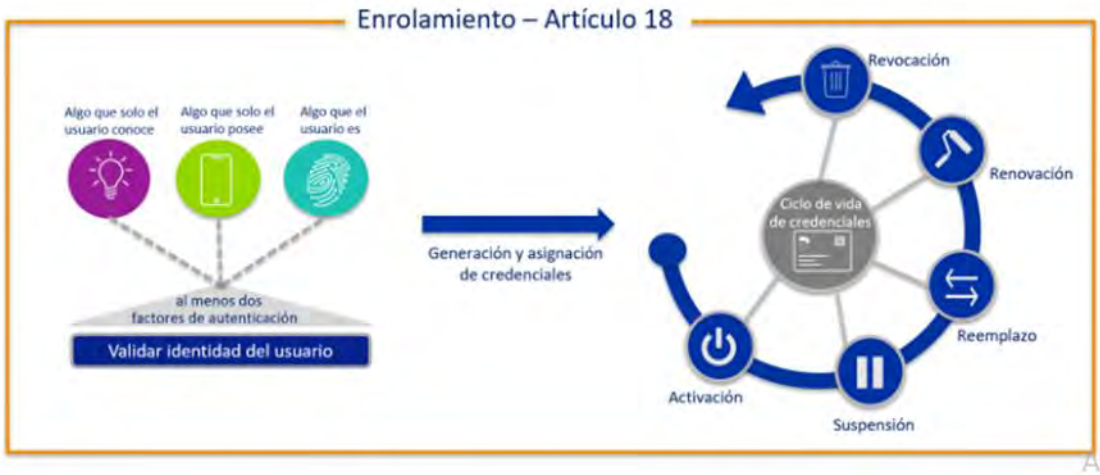
A partir de ello, se desprende que existe un gran margen de responsabilidad de las ESF por operaciones defectuosas o que no han sido reconocidas por los usuarios. Situación que podría incentivar, a su vez, al fraude por parte de los propios consumidores financieros al no reconocer las operaciones que realizan.

IV.2. Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado mediante la Resolución SBS N° 504-2021

Como bien sabemos, para realizar una operación de compra mediante un canal digital, resulta necesario que previamente nos hayamos registrado en el sistema, situación a la cual se denomina enrolamiento. En efecto, de acuerdo con Indecopi, en la Resolución N° 0107-2024/SPC-INDECOPI, se entiende como enrolamiento a aquella afiliación que se haya realizado a la plataforma de banca móvil donde se vayan a realizar las operaciones.

Al respecto, sin perjuicio del canal digital (banca móvil) indicado por Indecopi, de acuerdo con el artículo 18 del RGSIC, el enrolamiento de un usuario en un canal digital requiere por lo menos de lo siguiente: (I) verificar la identidad del usuario y tomar medidas para reducir posibilidad de suplantación, lo que incluye el uso de dos factores biométricos o el uso de dos factores de categorías diferentes; y (b) generar las credenciales y asignarlas al usuario, las cuales de acuerdo con la SBS, comprenden “contar con procedimientos para su activación, suspensión, reemplazo, renovación y revocación; además de, asegurar su confidencialidad e integridad” (2021, s/p).

Figura 3



Nota: Fuente Boletín SBS, julio 2022. A través de esta figura se visualiza gráficamente en lo que consiste el enrolamiento.

Ahora bien, luego del enrolamiento, el usuario procederá a realizar la operación que desea, para lo cual tendrá que pasar por el proceso de autenticación. Para ello, previamente, de acuerdo con el artículo 17 del RGSIC, las ESF deberán determinar las medidas que adoptarán respecto a (I) el o los factores de autenticación que serán requeridos; (II) los estándares criptográficos vigentes; (III) plazos y condiciones en las que será obligatorio que el usuario se vuelva a autenticar; (IV) la línea base de controles de seguridad de la información para prevenir las amenazas a las que esté expuesto el proceso de autenticación; (V) lineamientos para la retención de registros de auditoría para la detección de amenazas conocidas y eventos de seguridad de la información. Una vez determinado ello, se desprende que las ESF deberán implementar procesos de **autenticación para controlar el acceso a los servicios que provean a los usuarios por canales digitales**, sobre lo cual resulta importante indicar que, de acuerdo con la definición en el artículo 2 literal d) del RGSIC, **no se realiza distinción alguna sobre el tipo de canal digital; es decir, ya sea en comercio electrónico, banca por internet y/o banca móvil.**

Es de esta manera que, de acuerdo con el artículo 19 del RGSIC, se requerirá la **autenticación reforzada** para aquellas operaciones a través de un canal digital que impliquen pagos o transferencias de fondos a terceros. Es así como, aquella autenticación reforzada consiste en adoptar, se entiende que de forma conjunta, las siguientes medidas: (I) la utilización de una combinación de **factores de**

autenticación que, por lo menos, correspondan a dos categorías distintas y que sean independientes uno del otro; (II) contar con un control ante ataques de *The Man in the Middle*, el cual de acuerdo con IBM, es entendido como "un ciberataque en el que un pirata informático roba información confidencial al espiar las comunicaciones entre dos objetivos en línea, como un usuario y una aplicación web" (s/f, s/p). Asimismo, (III) cuando la operación sea exitosa, se debe notificar los datos de la operación al usuario.

Sin perjuicio de ello, existirán determinadas situaciones en que las ESF estarán exentas de realizar la autenticación reforzada, excepto la notificación, **de las operaciones realizadas por canales digitales**: (I) cuando las operaciones se realicen en favor de un beneficiario registrado previamente por el usuario como beneficiario de confianza; y (II) cuando las operaciones se realicen en favor del mismo usuario, siempre que sus cuentas se mantengan en la misma ESF.

Ahora bien, en la misma línea que el Reglamento de Tarjetas ha adoptado, el Reglamento de Ciberseguridad, a partir de la modificación introducida por la Resolución SBS N° 2286-2024, indica que las ESF serán responsables de las pérdidas de las operaciones no reconocidas por los usuarios efectuadas de las siguientes maneras: (I) por el canal digital sin cumplir con el requisito de autenticación reforzada, (II) en aplicación de la exención señalada en el artículo 20 numeral 2 del RGSIC, o (III) que han sido realizadas luego de que el usuario reportara el robo o pérdida de sus credenciales. Es así que, la única forma de que las ESF no sean responsables por las pérdidas derivadas de las operaciones no reconocidas por el canal digital es que puedan acreditar la responsabilidad del usuario.

IV.3. Reglamento de la Gestión de Conducta de Mercado del Sistema Financiero, aprobado mediante la Resolución SBS N° 3274-2017

El Reglamento de Conducta tiene incidencia en el tema que se pretende abordar, primero, porque busca regular las exigencias adecuadas de conducta de las ESF respecto de sus usuarios, en la oferta de productos financieros, en la ejecución de las prestaciones y en la atención de los reclamos. Segundo, a partir de la publicación de la Resolución SBS N° 2286-2024, se ha establecido además que las ESF, además, en el marco de las contrataciones de servicios financieros

mediante canales digitales, deberán tener en cuenta lo regulado en el Reglamento de Ciberseguridad.

Es así como, de acuerdo con el artículo 49 numeral 1 del RGC, para efectos de la contratación de productos y servicios financieros, las ESF deben considerar lo siguiente: (I) verificar la identidad del cliente y dejar constancia de la aceptación del contrato, lo cual incluye la hoja resumen o cartilla de información; (II) **para la celebración del contrato y durante su ejecución a través de canales digitales, deberá aplicar lo establecido en el Reglamento de Ciberseguridad**; y (III) pueden implementarse factores de autenticación como, por ejemplo, dispositivos físicos o virtuales en posesión del cliente, su firma manuscrita, huella digital, clave de identificación, firma o certificado digital, medios biométricos, entre otros.

A partir de ello, se desprende que el Reglamento de Conducta está dirigido a sentar las bases de la contratación de prestaciones financieras, sin realizar distingo entre los canales por los cuales se realizará la prestación, así como busca afianzar la seguridad de la identidad de los usuarios que contratan mediante métodos de autenticación.

IV.4. Código de Protección y Defensa del Consumidor, Ley N° 29571

Como es de conocimiento, en el marco de un contrato de consumo, específicamente el de consumo financiero, las ESF tienen la facultad de redactar unilateralmente las cláusulas generales de contratación, frente al consumidor quien solo tendrá la facultad de elegir con quién contratar. Es así como, la ESF detenta un poder mayor frente al consumidor, quien no tendrá la facultad de negociar el contenido de un contrato de consumo, como sí sucede en los contratos paritarios. En esa misma línea, las ESF gozan de una mayor *expertise* y conocimiento sobre los productos financieros que ofrecen y, por ende, los riesgos que pueden derivar de aquel. De ahí que, a las relaciones de consumo le es inherente la asimetría informativa, y para restablecer o equilibrar esta relación, las ESF tienen la obligación de cumplir con el deber de idoneidad e información.

Específicamente, a efectos de entender las imputaciones de responsabilidad administrativas de las ESF que se analizarán con posterioridad, resulta

importante desarrollar el deber de idoneidad. Este, acorde con el artículo 18 del CPDC, es el deber por el que responde la ESF sobre la idoneidad del producto ofrecido, la cual es definida, en el artículo 19 del CPDC, como “la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe, en función a lo que se le hubiera ofrecido [...]”. Es así como, para determinar si se ha cumplido o no con la idoneidad del producto, el artículo 20 del CPDC indica que “debe compararse el mismo con las garantías que el proveedor está brindando y a las que está obligado. Las garantías son las características, condiciones o términos con los que cuenta el producto o servicio”. Estas garantías pueden ser legales, explícitas o implícitas.

Es así como, resulta importante aludir a las garantías legales, las cuales como se indica en el literal a) del artículo 20 del CPDC, es considerada como tal “cuando por mandato de la ley o de las regulaciones vigentes no se permite la comercialización de un producto o la prestación de un servicio, sin cumplir con la referida garantía”. En ese sentido, las garantías legales implican el cumplimiento de las obligaciones de las ESF reguladas en diversos dispositivos normativos como parte de las condiciones en las prestaciones de sus productos financieros. Específicamente, en el caso de operaciones con tarjetas de débito y/o crédito, las garantías legales principalmente serían las disposiciones señaladas en los Reglamentos de Tarjetas de Crédito y Débito, el Reglamento de Ciberseguridad, el Reglamento de Conducta.

Tener en cuenta ello resulta importante para los consumidores financieros pues les permitirá, a su vez, poder exigir la efectiva prestación de producto financiero contratado, sobre todo si los intereses involucrados son el ahorro del público, la capacidad de pago y/o situación crediticia. Asimismo, si bien es cierto que, como indica Maraví, muchos de los problemas que surgen del deber de idoneidad “versan sobre la falta de coincidencia entre lo que un consumidor espera y lo que realmente recibe, tomando en cuenta la cantidad y calidad de la información que ha recibido” (citado en Quinteros, 2018, p.366). Esta brecha, en principio, desaparece cuando la expectativa del consumidor se alínea con las obligaciones de las ESF que no permiten margen de interpretación extensiva, lo cual resulta siendo más objetiva.

Este es el caso de las obligaciones de las ESF sobre las medidas de seguridad en la contratación y en las operaciones con tarjetas de crédito y/o débito. En efecto, de acuerdo con el estàndar establecido por el Indecopi en la Resolución N° 0107-2024, “en las expectativas razonables de un consumidor, al contar con un producto financiero con las ESF, 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 no idóneo”.

V. ANÁLISIS DE LOS CRITERIOS DE LAS RESOLUCIONES ADMINISTRATIVAS DE INDECOPI SOBRE LA RESPONSABILIDAD ADMINISTRATIVA DE LAS ESF

Una vez expuestas las obligaciones de las ESF respecto a las operaciones no reconocidas con tarjeta presente y no presente, a través de los canales digitales. Resulta importante analizar las posiciones tanto de Indecopi como de la SBS respecto a la responsabilidad administrativa de las ESF por el incumplimiento de aquellas medidas. Para ello, se desarrollará y expondrá el análisis de las resoluciones administrativas que engloban esta problemática. De esta manera, se podrá determinar en el siguiente apartado la posible afectación al principio de confianza legítima por la divergencia de posiciones.

V.1. Análisis de la responsabilidad administrativa de las ESF por operaciones con tarjeta de crédito y/o débito en banca por internet y/o banca móvil

Mediante la Resolución N° 0283-2024/SPC-INDECOPI, Indecopi confirmó la resolución apelada que declaró fundada la denuncia interpuesta por Rosalía Illa Choque contra Mibanco, al probarse que no cumplió con adoptar las medidas de seguridad de 3 operaciones por el monto de S/ 14,099. De los hechos se deslinda que la denunciante advirtió que se habían producido 3 operaciones que no había realizado con cargo a su cuenta de ahorros, quedándole así solo S/ 4,000. Ante ello, inmediatamente llamó a la denunciada para que realice el bloqueo de su tarjeta; no obstante, no se realizó el bloqueo de sus cuentas. Cabe indicar además que, la tarjeta de crédito del denunciante se encontraba activa al

momento en que se realizaron las operaciones. A continuación, se puede visualizar la fecha, hora y el monto de cada operación no reconocida:

FECHA	HORA	TIPO DE OPERACIÓN	MONTO S/
1-10-2022	13:59:13	Transferencia a cuenta	5 000,00
1-10-2022	14:09:43	Transferencia a cuenta	5 000,00
1-10-2022	14:04:05	Pago de servicios	4 099,00

Al respecto, el razonamiento de la Sala Especializada en Protección al Consumidor fue el siguiente: primero, analizar si la ESF cumplió con su deber de monitoreo y detección de operaciones inusuales. Para ello, indicó que, de acuerdo a lo que se entiende por comportamiento habitual de consumo, acorde con el artículo 2 numeral 5 del RTCD[2]; así como, el deber de las ESF sobre la implementación de medidas de seguridad respecto a operaciones que no corresponden con el comportamiento habitual de consumo del usuario, de acuerdo con el artículo 17 del RTCD, se determinaría el comportamiento habitual del usuario mediante el importe individual de las operaciones que el consumidor usualmente realizaba con el producto objeto de denuncia, lo cual permitirá conocer si es una operación inusual o no.

Ante ello, la Sala concluye que la ESF no se encontraba obligada a efectuar las medidas de seguridad sobre operaciones inusuales, ya que se advierte los montos de las operaciones cuestionadas son menores respecto a la transferencia máxima realizada ascendente a S/ 24,998.50 que se había registrado en su historial; por lo tanto, se consideraba un comportamiento habitual de consumo.

Segundo, la Sala analizó si las operaciones materia de denuncia fueron autorizadas correctamente; es decir, la validez de las operaciones. Al respecto, indicó que en el presente caso resultaba aplicable el Reglamento de Ciberseguridad, ya que las operaciones cuestionadas se realizaron en banca por internet. Asimismo, indicó que, pese a que la ESF haya implementado los factores de autenticación, se habría incumplido el artículo 19 del Reglamento de Ciberseguridad en relación a los métodos de autenticación reforzada en canal

[2] "el tipo de operaciones que usualmente realiza cada usuario con sus tarjetas, considerando diversos factores, como por ejemplo el país de consumo, tipos de comercio, frecuencia, canal utilizado, entre otros, los cuales se determinan a partir de la información histórica que registra la ESF".

digital, ya que, por un lado, de los medios probatorios, no se apreció que efectivamente se dio el ingreso válido a la plataforma del banco, ni que se cumplió con ingresar las claves dinámicas para la validación de las operaciones. Por otro lado, no se apreció que se haya atribuido un código de autenticación mediante métodos criptográficos a cada una de las operaciones cuestionadas. Además, no se demostró que la ESF le haya notificado a la denunciante la realización exitosa de cada operación. Por lo tanto, al no cumplir con la garantía legal, se incumplió el deber de idoneidad.

Mediante la Resolución N° 0107-2024/SPC-INDECOPI, Indecopi confirmó la resolución apelada que declaró fundada la denuncia interpuesta por María Cansaya Mamani contra Scotiabank, al probarse que no adoptó las medidas de seguridad pertinentes cuando se efectuaron operaciones por el monto de S/ 19,383.62. De los hechos se deslinda que la denunciante advirtió que se habían producido 3 operaciones que reconocía, luego de una llamada de Scotiabank preguntándole si las reconocía. A continuación, se puede visualizar la fecha, hora y el monto de cada operación no reconocida:

FECHA	CONCEPTO	IMPORTE
07/09/2022	Transferencia Inmed. CCE línea	S/6 458,52
07/09/2022	Transferencia Inmed. CCE línea	S/6 461,54
07/09/2022	Transferencia Inmed. CCE línea	S/6 463,56
	Monto total	S/19,383.62

Al respecto, el razonamiento de la Sala Especializada en Protección al Consumidor fue el siguiente: primero, analizar si la ESF cumplió con su deber de monitoreo y detección de operaciones inusuales. Para ello, en la misma línea de la resolución previamente analizada, la Sala consideró que de acuerdo con el artículo 2 numeral 5 y el artículo 17 del RTCD[3], se determinaría el comportamiento habitual del usuario mediante el importe individual de las operaciones que el consumidor usualmente realizaba con el producto objeto de denuncia, a efectos de conocer si es una operación inusual o no.

[3] "el tipo de operaciones que usualmente realiza cada usuario con sus tarjetas, considerando diversos factores, como por ejemplo el país de consumo, tipos de comercio, frecuencia, canal utilizado, entre otros, los cuales se determinan a partir de la información histórica que registra la ESF".

Ante ello, la Sala concluye que las operaciones cuestionadas son mayores respecto a la transferencia máxima realizada ascendente a S/ 5,000 que se había registrado en su historial; por lo tanto, al estar frente a una operación inusual, la ESF tenía la obligación de emitir alerta en la primera operación realizada del monto de S/ 6,458.52, a efectos de adoptar las medidas necesarias para evitar que se continúen realizando las próximas operaciones no reconocidas.

Segundo, la Sala analizó si las operaciones materia de denuncia fueron autorizadas correctamente; es decir, la validez de las operaciones. Al respecto, indicó que en el presente caso resultaba aplicable el Reglamento de Ciberseguridad, ya que las operaciones cuestionadas se realizaron en banca móvil.

Ahora bien, durante el análisis resultó importante el análisis del enrolamiento de la denunciada a la banca móvil, ya que afirmó que nunca habría utilizado canales virtuales para realizar operaciones. Al respecto, la Sala determinó que la denunciada sí se encontraba afiliada a la banca móvil, conforme a los medios probatorios presentados por la ESF[4]; por lo tanto, sí se encontraba habilitada para realizar operaciones a través de la banca móvil.

Sin embargo, se advirtió que las operaciones cuestionadas fueron posibles mediante el uso de la opción biométrica, y sobre lo cual la ESF no presentó medio probatorio fehaciente que pudiera demostrar que la denunciante se había afiliado a ese mecanismo; por lo tanto, las operaciones no habrían sido realizadas por ella. Por lo tanto, al no verificarse que se llevó adecuadamente el enrolamiento, de acuerdo con el artículo 18 del Reglamento de Ciberseguridad, no se cumplió con la garantía legal y, por ende, el deber de idoneidad.

A partir de lo expuesto en las resoluciones administrativas, se puede advertir, por un lado, que las ESF únicamente tendrán la obligación de emitir alertas sobre las operaciones que sean consideradas inusuales; es decir, aquellas que registren operaciones por encima del monto máximo habitual del usuario que se haya registrado en la ESF. Por otro lado, se advierte que para las operaciones

[4] (I) Impresión de pantalla del reporte denominado “consulta clientes JOY”, (II) impresión del reporte de su sistema “Status Clave Digital”; (III) registro con ID 2001000002481853; (IV) afiliación del celular a la clave digital y la afiliación del correo electrónico a la referida clave digital.

por banca por internet y/o banca móvil resultan aplicables el Reglamento de Ciberseguridad; por lo tanto, las ESF tendrán que demostrar que han implementado medidas de enrolamiento y autenticación reforzada, pero que además hayan sido efectivamente utilizadas.

Asimismo, otro aspecto importante que se desprende de las resoluciones administrativas es que, al momento de analizar la aplicación del Reglamento de Ciberseguridad, se indica que, si bien resultan aplicables para operaciones realizadas a través de la banca por internet y la banca móvil, no es así para las realizadas por comercio electrónico, puesto sobre este supuesto aún existen controversias.

V.2. Análisis de la responsabilidad administrativa de las ESF por operaciones con tarjeta de crédito y/o débito en establecimientos presenciales

Mediante la Resolución N° 0003-2024/SPC-INDECOPI, Indecopi confirmó la resolución apelada que declaró fundada la denuncia interpuesta por Denis Garcia Neyra contra Mibanco, al probarse que no cumplió con adoptar las medidas de seguridad de operaciones por el monto de S/ 17,116. De los hechos se deslinda que se habría retirado el dinero de la cuenta de ahorros del denunciante por el monto indicado.

Al respecto, el razonamiento de la Sala Especializada en Protección al Consumidor fue el siguiente: primero, analizar si la ESF cumplió con su deber de monitoreo y detección de operaciones inusuales. Para ello, en la misma línea de la resolución previamente analizada, la Sala consideró que de acuerdo con el artículo 2 numeral 5 y el artículo 17 del RTCD[5], se determinaría el comportamiento habitual del usuario mediante el importe individual de las operaciones que el consumidor usualmente realizaba con el producto objeto de denuncia, a efectos de conocer si es una operación inusual o no.

No obstante, se advirtió que la operación cuestionada habría sido la primera realizada con aquella cuenta; por lo tanto, no se contaba con un historial de

[5] "el tipo de operaciones que usualmente realiza cada usuario con sus tarjetas, considerando diversos factores, como por ejemplo el país de consumo, tipos de comercio, frecuencia, canal utilizado, entre otros, los cuales se determinan a partir de la información histórica que registra la ESF".

registro de operaciones para verificar el patrón de consumo. Sin perjuicio de ello, la Sala consideró que se estaba ante una operación inusual pues el retiro fue del 100%; por lo tanto, la ESF tenía la obligación de adoptar medidas de seguridad para corroborar la validez del retiro del efectivo, mas no lo hizo.

Segundo, la Sala indicó que se analizaría si la operación cuestionada era válida; sin embargo, no pudo realizarlo; debido a que la ESF no presentó medios probatorios para demostrarlo. Por lo tanto, al no haber cumplido con las disposiciones del RTCD, no se cumplió con la garantía legal y, por ende, el deber de idoneidad.

Mediante la Resolución N° 0102-2024/SPC-INDECOPI, Indecopi confirmó la resolución apelada que declaró fundada la denuncia interpuesta por Juan Arrisueño Barreto contra Interbank, al probarse que no cumplió con adoptar las medidas de seguridad de operaciones por el monto de S/ 30,248.69. A continuación, se puede visualizar la fecha, hora y el monto de cada operación no reconocida:

Fecha	Hora	Descripción	Monto
26/06/2022	11:26:33	Compra POS	S/ 24 643,00
26/06/2022	11:31:26	Retiro con tarjeta	S/ 2 500,00
26/06/2022	11:32:34	Retiro con tarjeta	S/ 3 105,60 (US$ 800,00)
TOTAL: S/ 30 248,60			

Al respecto, el razonamiento de la Sala Especializada en Protección al Consumidor fue el siguiente: primero, analizar si la ESF cumplió con su deber de monitoreo y detección de operaciones inusuales. Para ello, en la misma línea de la resolución previamente analizada, la Sala consideró que de acuerdo con el artículo 2 numeral 5 y el artículo 17 del RTCD[6], se determinaría el comportamiento habitual del usuario mediante el importe individual de las operaciones que el consumidor usualmente realizaba con el producto objeto de denuncia, a efectos de conocer si es una operación inusual o no.

[6] "el tipo de operaciones que usualmente realiza cada usuario con sus tarjetas, considerando diversos factores, como por ejemplo el país de consumo, tipos de comercio, frecuencia, canal utilizado, entre otros, los cuales se determinan a partir de la información histórica que registra la ESF".

Ante ello, la Sala concluye que las operaciones cuestionadas son mayores respecto a la transferencia máxima realizada ascendente a S/ 2,732 que se había registrado en su historial; por lo tanto, al estar frente a una operación inusual, la ESF tenía la obligación de emitir alerta en la primera operación realizada del monto de S/ 24,643, a efectos de adoptar las medidas necesarias para evitar que se concreten las demás.

Segundo, la Sala analizó únicamente si la primera operación cuestionada que se realizó en un centro comercial sería válida. Para ello, requirió verificar si la operación se realizó con el uso conjunto del medio de pago y la clave secreta u otro método de autenticación; así como, si de acuerdo con el artículo 14 del RTCD, se emitió la orden de pago respectiva autorizada por el usuario. Al respecto, la ESF demostró la orden de pago que evidencia que la operación fue aprobada mediante el uso de clave y se consignó el DNI y firma del usuario.

No obstante, pese a lo expuesto, la Sala determinó que la ESF tenía responsabilidad por la operación no reconocida ya que no implementó las medidas de seguridad cuando se realizó la primera operación que fue calificada como operación inusual. Por lo tanto, al no haber cumplido con las disposiciones del RTCD, no se cumplió con la garantía legal y, por ende, el deber de idoneidad.

Debido a lo expuesto, se puede deslindar, por un lado, que al igual que en las operaciones mediante banca móvil y/o por internet, las ESF únicamente tendrán la obligación de emitir alertas sobre las operaciones que sean consideradas inusuales; es decir, aquellas que registren operaciones por encima del monto máximo habitual del usuario que se haya registrado en la ESF. Por otro lado, para las operaciones con tarjetas de débito y/o crédito en establecimientos presenciales, la regulación aplicable es el Reglamento de Tarjetas, mas no la de Ciberseguridad.

V.3. Análisis de la responsabilidad administrativa de las ESF por operaciones con tarjeta de crédito y/o débito en comercio electrónico

Las operaciones que se realizan mediante comercio electrónico han sido, en estos últimos meses, objeto de gran debate; debido a que, siguen una línea argumentativa distinta de acuerdo con la postura de Indecopi y la SBS. En efecto,

a diferencia de la claridad sobre la norma jurídica aplicable para las operaciones realizadas con tarjeta de débito y/o crédito en establecimientos comerciales presenciales o en banca móvil y/o banca por internet, en las operaciones realizadas por comercio electrónico, se torna difuso; debido a la asunción de responsabilidad que ello implicaría, pues se encuentran diversos actores involucrados en el procesamiento de pagos. Para explicitar la controversia, resulta necesario desarrollar y analizar las siguientes resoluciones administrativas.

Mediante la Resolución N° 0338-2024/SPC-INDECOPI, Indecopi confirmó la resolución apelada que declaró fundada la denuncia interpuesta por Nasha Soledad Valdivia Esquerre contra el Banco de Crédito del Perú, al probarse que no cumplió con adoptar las medidas de seguridad de operaciones, al permitir que se realicen 8 operaciones no reconocidas, con cargo en la cuenta de ahorro del denunciante, a través de la plataforma de Agora (comercio electrónico). A continuación, se puede visualizar la fecha, hora y el monto de cada operación no reconocida:

HORA	ESTABLECIMIENTO	IMPORTE CARGADO EN DÓLARES	CONVERSIÓN A SOLES
15:07:38	Agora	US$ 273,97	S/ 1 000,00
15:14:38	Agora	US$ 540,54	S/ 2 000,00
15:17:34	Agora	US$ 540,54	S/ 2 000,00
15:18:19	Agora	US$ 540,54	S/ 2 000,00
15:19:39	Agora	US$ 540,54	S/ 2 000,00
15:20:31	Agora	US$ 540,54	S/ 2 000,00
15:23:24	Agora	US$ 540,54	S/ 2 000,00
15:24:40	Agora	US$ 540,54	S/ 2 000,00
TOTAL			US$ 4 057,75

Ante ello, la Sala Especializada en Protección al Consumidor concluyó que era necesario realizar un análisis sobre la aplicación o no del RGSIC en el presente caso que engloba una operación no reconocida realiza con la tarjeta de crédito de la denunciante en el que el emisor es el Banco de Crédito del Perú, y se realizó a través de Agora que es considerado un comercio electrónico.

Al respecto, **la Sala consideró que la definición de "canal digital" aludido en el RGSIC, únicamente refiere a las plataformas a través de las cuales el**

usuario puede efectuar un previo enrolamiento con anterioridad a la realización de cualquier operación y que permita efectuar alguna de las operaciones detalladas en el artículo 19 del reglamento aludido. Por lo tanto, indicó que el RGSIC solo es aplicable a las operaciones que se realizan en banca móvil, banca por internet, billeteras digitales.

Es así como, en el caso en concreto, al realizarse las operaciones no reconocidas a través de una plataforma de Agora, que es considerada como un comercio electrónico, entonces no resulta aplicable el RGSIC para efectos de imputar responsabilidad administrativa al Banco de Crédito del Perú. Es decir, el denunciado no tenía la obligación de cumplir con las medidas señaladas en RGSIC, ya que la operación no reconocida se realizó en un comercio electrónico. En efecto, a través del fundamento 11, Indecopi expresamente señala que "aun cuando para acceder a la plataforma de Agora existió un enrolamiento previo efectuado por el cliente, lo cierto es que su monitoreo y/o validación de seguridad no son responsabilidad de la entidad financiera, sino del establecimiento comercial".

En consecuencia, el análisis en el presente caso para imputar la responsabilidad administrativa del denunciado, únicamente se ciñe en las obligaciones derivadas del Reglamento de Tarjetas, para efectos de concluir si cumplió o no con la garantía legal y, por ende, el deber de idoneidad, de conformidad con las disposiciones del CPDC que en un anterior apartado se ha explicado.

Específicamente, indica que el análisis para imputar la responsabilidad aludida reside en verificar el cumplimiento del deber de monitoreo, así como de las medidas para catalogar a la operación como válida. Al respecto, la Sala consideró que existía responsabilidad del denunciado, pues si bien había presentado los medios probatorios para catalogar las operaciones como válidas, las claves dinámicas enviadas por mensaje de texto al denunciante para efectos de concretar las operaciones, no permiten concluir que tienen relación alguna estas.

Por otro lado, otra resolución que resulta relevante a efectos de contrastar la posición difusa respecto a las operaciones con tarjetas a través del comercio electrónico es la Resolución N° 0249-2024/SPC-INDECOPI. En esta, la Sala

Especializada en Protección al Consumidor levantó la suspensión de procedimiento seguido por Edwin Pacheco Quinto con Scotiabank, el cual se había iniciado en la Comisión de Protección de Sede Junín. Esta suspensión se debió a que la Sala solicitó información técnica a la SBS en relación a la aplicación del RGSIC en canales digitales. Cabe indicar que, si bien la controversia no es por una operación realizada con tarjeta a través de un comercio electrónico, sino por el desembolso de un préstamo por la suma de S/ 14,932.80, y por las transferencias de las sumas S/ 14,300, S/ 3,500, S/99, las preguntas formuladas para la absolución de la SBS resultan pertinentes para dilucidar la posición de la SBS al respecto.

En efecto, mediante Oficio Nº 01690-2024-SBS, emitido el 11 de enero de 2024, la SBS responde aludiendo a la interpretación de las disposiciones del RGSIC. Para efectos del presente trabajo, entre los principales pronunciamientos se encuentran los siguientes:

1. "Los canales como **comercios electrónicos**, POS, cajeros automáticos y similares, a través de los cuales las entidades financieras proveen sus servicios a los usuarios, **son considerados canales digitales**".
2. "Las **empresas del sistema financiero son responsables de autenticar la identidad del usuario** cuando este instruya transacciones que lo requieran, como el pago de servicios, **tanto en canales propios como de terceros**".
3. "La **autenticación reforzada en caso se realice una operación de pago en un comercio electrónico se efectúa mediante los factores de autenticación que la entidad financiera implemente y ponga a disposición de los usuarios**. En una situación común, el primer factor podría consistir en los datos contenidos en la tarjeta, los cuales son registrados por el usuario en la página web o App del comercio electrónico; el segundo factor, podría ser omitido por la entidad, bajo su responsabilidad, conforme a las condiciones establecidas para la exención de autenticación reforzada en el artículo 20 de RGSIC; de lo contrario, aplicaría el segundo factor".

4. El **RGISC “no es aplicable a la afiliación** (creación de usuario y/o contraseña) **que se efectúa en determinados comercios electrónicos antes de efectuar compras y/o acceder a servicios de este**”.

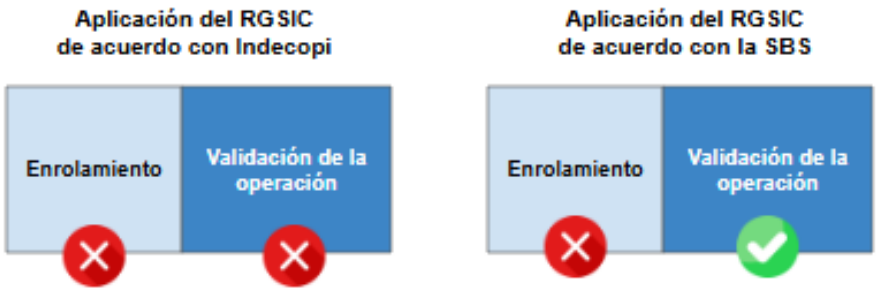
   (El subrayado y el resaltado es mío)

Ante ello, se desprende que en la definición de “canales digitales” que se alude en el RGSIC, también se incluyen a los comercios electrónicos a través de los cuales se realizan operaciones con tarjetas. En ese sentido, si bien es cierto que el RGSIC no se aplica a los enrolamientos (procesos de afiliación) en las plataformas de los comercios electrónicos, sí resulta aplicable para las operaciones de compra que se realizan a través de estos. Situación que guarda concordancia al indicarse que las ESF son responsables de autenticar la identidad de los usuarios cuando el titular instruya transacciones, tanto en canales propios como de terceros; es decir, en banca por internet y/o banca móvil, y comercios electrónicos, respectivamente.

Es así como, podemos evidenciar el contraste existente de la posición de la SBS, a través del Oficio aludido, y la posición de Indecopi, a través de la Resolución N° 0249-2024/SPC-INDECOPI. En efecto, mientras que, la SBS indica que las ESF tienen la obligación de aplicar el RGSIC para efectos de en autenticar la identidad de los usuarios que realizan operaciones con tarjeta no solo a través de banca por internet y/o banca móvil, sino además a través del comercio electrónico, entre otros canales digitales, excluyendo su aplicación en el proceso de enrolamiento.

Por el contrario, Indecopi ha indicado que el RGSIC es únicamente aplicable para operaciones que se realizan por banca por internet y/o por banca móvil, y no por otros canales como, por ejemplo, comercio electrónico, ya que los primeros son las únicas plataformas en donde las ESF proveen tanto el proceso de enrolamiento como el ordenamiento de las operaciones.

Figura 4



Nota: Fuente, elaboración propia. A través de esta figura se visualiza gráficamente las posiciones de Indecopi y SBS en relación a la aplicación del RGSIC en operaciones con tarjetas a través de comercio electrónico.

VI. ANÁLISIS DE LA VULNERACIÓN DEL PRINCIPIO DE CONFIANZA LEGÍTIMA POR LAS POSICIONES CONTRARIAS EN RELACIÓN A LA APLICACIÓN DEL RGSIC EN LAS OPERACIONES NO RECONOCIDAS A TRAVÉS DE COMERCIO ELECTRÓNICO

VI.1. Desarrollo del principio de confianza legítima y su relación con el principio de seguridad jurídica

El principio de confianza legítima es conocido como el principio de la confianza a la administración. Una de las primeras sentencias referidas a la vulneración de este principio fue emitida, en 1973, por el Tribunal de Justicia de la Unión Europea, mediante el cual se declaró que la Comisión Europea la había vulnerado, pues habría aprobado dispositivos normativos a través del cual aumentaba los salarios de sus funcionarios; no obstante, posteriormente emitió el Reglamento N° 2647/72, a través del cual se adaptan las retribuciones y pensiones de los funcionarios. Por ende, se solicitó la anulación parcial de este reglamento, teniendo entre sus fundamentos la vulneración del principio de confianza legítima, pues la Administración al contradecir su actuación sobre el aumento de salarios de los funcionarios, generó expectativas sobre estos.

Es en esta misma línea que, en el Perú, se ha regulado el principio de confianza legítima a través del artículo IV numeral 1.15 del Título Preliminar del TUO de la LPAG, de la siguiente manera:

> “La autoridad administrativa brinda a los administrados o sus representantes información veraz, completa y confiable sobre cada procedimiento a su cargo, de modo tal que, en todo momento, **el administrado pueda tener una comprensión cierta sobre los requisitos, trámites, duración estimada y resultados posibles que se podrían obtener.**
>
> **Las actuaciones de la autoridad administrativa son congruentes con las expectativas legítimas de los administrados razonablemente generadas por la práctica y los antecedentes administrativos**, salvo que por las razones que se expliciten, por escrito, decida apartarse de ellos.
>
> La autoridad administrativa se somete al ordenamiento jurídico vigente y no puede actuar arbitrariamente. En tal sentido, la autoridad administrativa no puede variar irrazonable e inmotivadamente la interpretación de las normas aplicables”.

De acuerdo con ello, se desprende que el principio de confianza legítima alude a la generación de confianza que la Administración debe brindar a los administrados, sobre las actuaciones que estos deben seguir o sobre los posibles resultados que puedan obtener, a partir del actuar de la Administración, ya sea a través de resoluciones administrativas de forma reiterada o a través de precedentes vinculantes.

En efecto, mediante Exp. N° 02793-2022-PA/TC, en alusión a la vulneración de este principio, el TC ha indicado que “el recurrente no pudo tener una comprensión cierta sobre los requisitos, etapas y duración estimada de estas, y del acto que concretaba la presentación de la solicitud, al no contar con información certera y completa a partir de lo establecido”. Asimismo, que “la ausencia o insuficiente esclarecimiento [...] y razonabilidad de las reglas procedimentales [...] afectó su derecho”.

Por lo tanto, se desprende que, se afecta el principio de confianza legítima o predictibilidad cuando el administrado no tiene claro cómo debe concretar su actuar como consecuencia a la diversidad de posiciones de la Administración.

Situación que deviene en la posible imputación de responsabilidades por parte del administrado, que claramente lo termina perjudicando.

Cabe indicar además que, este principio, a su vez, está íntimamente relacionado con el principio de seguridad jurídica, Este tal como señala el TC, mediante el Exp. N° 0016-2002-AI/TC, si bien no tiene un reconocimiento constitucional, se desprende que es inherente a todo Estado de Derecho, y se puede entender desde dos dimensiones: la objetiva y la subjetiva. La primera exige a los poderes públicos que sea coherente y propicie confianza en el ciudadano, basado en el actuar predecible de la Administración. La segunda implica que los administrados puedan dirigir su actuar presente y futuro y, por ende, el cumplimiento de sus obligaciones confiando en la garantía del actuar de la Administración.

Es así como, el actuar de la Administración debe estar dirigido de forma clara y precisa; ya sea a través de los precedentes vinculantes o criterios reiterados sobre una posición que permitan a los administrados poder conocer las obligaciones que deben cumplir, así como las consecuencias jurídicas que derivan de su incumplimiento. No obstante, en una situación contraria, claramente les generaría inseguridad jurídica sobre cómo dirigir su actuar.

VI.2. Análisis de la posible afectación del principio de confianza legítima y seguridad jurídica en la imputación de la responsabilidad administrativa de las ESF por operaciones no reconocidas a través del comercio electrónico

Como se ha desarrollado previamente, el principio de confianza legítima o predictibilidad y la seguridad jurídica están estrechamente unidos por la implicancia que tiene en el actuar de la Administración y de los administrados.

Ahora bien, en el objeto materia de estudio, se ha evidenciado que Indecopi tiene los siguientes criterios sobre la aplicación del RGSIC en las operaciones realizadas con tarjetas: (i) el RGSIC no es aplicable para operaciones realizadas en canales presenciales, y tampoco en digitales siempre que no sean banca móvil y/o banca por internet; y (II) el RGSIC únicamente es aplicable para operaciones que se realicen en banca móvil y/o banca por internet.

Mientras que la SBS sobre la aplicación del RGSIC ha indicado que el RGSIC es aplicable en todo tipo de operaciones que se realiza a través de un canal digital, entre los cuales además de la banca por internet y/o banca móvil, también son considerados los POS, los comercios electrónicos, entre otros, a partir de lo cual concluye que el RGSIC es aplicable para todas las operaciones con tarjeta, incluyendo a las compras presenciales ya que se realizan por POS, y a los comercios electrónicos, excepcionalmente en la fase de enrolamiento.

Asimismo, se debe resaltar que, pese a que Indecopi tiene conocimiento de la interpretación sobre las disposiciones del RGSIC que la SBS le indica que debe considerar, a través del Oficio N° 1690-2024-SBS, emitido el 11 de enero de 2024, aquel ha hecho caso omiso sobre ello, como se puede evidenciar a partir de las resoluciones administrativas posteriores que emitió[7].

Por lo tanto, ante esta situación, podemos evidenciar que se afecta el principio de confianza legítima tanto de las ESF como de los consumidores financieros, pues no termina siendo clara en qué supuestos serán aplicables el RGSIC. Situación que terminaría derivando a las ESF a continuar con la comisión de infracciones administrativas por no tener claro las obligaciones que deben cumplir en relación al RGSIC en determinados tipos de operaciones con tarjetas.

Sin perjuicio de ello, con la promulgación de la Resolución SBS N° 02286-2024, parecería, en principio, paliar la vulneración al principio de confianza legítima. Al introducir en el Reglamento de Tarjetas, sin hacer distinción alguna sobre el canal digital, que las ESF deberán adoptar como mínimo, entre diversas medidas, las medidas de seguridad sobre el proceso de autenticación del usuario para efectuar operaciones, acorde a lo establecido en el artículo 19 del RGSIC.

VII. CONCLUSIONES

Primero, a partir del contexto que devino en la pandemia, y por la necesidad evidente del *contacless*, se evidenció un aumento de la población en la adopción de diversas modalidades del sistema de pagos: ya sea mediante billeteras digitales, banca móvil y residualmente el uso en efectivo. Asimismo, se evidenció

[7] Como, por ejemplo, Resolución N° 0283-2024/SPC-INDECOPI (Fecha 31 de enero de 2024); Resolución N° 0107-2024/SPC-INDECOPI (Fecha 15 de enero de 2024); Resolución N° 0102-2024/SPC-INDECOPI (Fecha 15 de enero de 2024); y Resolución N° 0338-2024/SPC-INDECOPI (Fecha 13 de febrero de 2024)

un aumento de productos financieros por parte de los minoristas no bancarizados: adquisición de tarjetas de débito y crédito.

Segundo, a partir del aumento de las transacciones en línea, ya sea a través de comercio electrónico, banca móvil y/o banca por internet, y compras presenciales a través de POS, en las que se han usado tarjetas de crédito y/o débito, los consumidores financieros se han encontrado expuestos a mayores riesgos, por fraude, clonación, phishing, entre otros riesgos.

Tercero, por el aumento del número de reclamos por operaciones no reconocidas, se publicó, en el 2021, el RGSIC el cual comenzó a regular las obligaciones de las ESF en relación a las medidas de ciberseguridad y en las medidas de seguridad en relación a la autenticación de la identidad de los usuarios con productos financieros por operaciones a través de canales digitales.

Cuarto, la línea argumentativa que ha seguido Indecopi en sus resoluciones administrativas, en relación a la aplicación del RGSIC, ha sido que este únicamente es aplicable para operaciones con tarjetas que se realicen en banca móvil y/o banca por internet. Contrariamente, la SBS ha indicado a través del Oficio N° 1690-2024-SBS que, el RGSIC es aplicable a las operaciones con tarjeta que se realizan a través de cualquier canal digital, en el que se incluye a los comercios electrónicos, excepcionalmente en la fase de enrolamiento.

Quinto, por las posiciones contrarias que han devenido ambas entidades públicas, se vulnera el principio de confianza legítima y seguridad jurídica, tanto de las ESF como de los consumidores, pues impide que estos puedan dirigir claramente su actuar para efectos de cumplir con sus obligaciones en materia de seguridad como para conocer los derechos que les corresponden o los riesgos a los que se encuentran expuestos, respectivamente. Sin perjuicio de ello, a partir de la promulgación de la Resolución SBS N° 02286-2024, se espera que se pueda paliar la vulneración a estos principios, pues establecen medidas mucho más claras en relación a la aplicación del RGSIC en las operaciones con tarjetas de crédito y/o débito sin hacer distinción alguna sobre el canal digital.

VIII. BIBLIOGRAFÍA

Asociación de Bancos del Perú (2024). Boletín Bancario, trimestre: 3-2024. Estadísticas del sector.

https://www.asbanc.com.pe/estadisticas-del-sector

Banco Central de Reserva del Perú (2024). Reporte de Estabilidad Financiera, mayo de 2024. Cuadro 7, p. 82

https://www.bcrp.gob.pe/docs/Publicaciones/Reporte-Estabilidad-Financiera/2024/mayo/ref-mayo-2024.pdf

Banco de Crédito del Perú (2024). Informes de Reclamos, 2024. https://www.viabcp.com/transparencia?rfid=footer:span-datatranslatetruetr:link:10

BBVA Perú (2024). Informes de Reclamos, 2024.

https://www.bbva.pe/personas/sos-cliente/estadisticas.html

Banco Internacional del Perú (2024). Informes de Reclamos, 2024.

https://interbank.pe/informacion-de-reclamos?tabs=tab-informacion

Código de Protección y Defensa del Consumidor (2 de septiembre de 2010). Normas Legales, Ley N° 29571. Diario Oficial El Peruano.

Espinoza, J. (2019). Derecho de la responsabilidad civil. Tomo I. Instituto Pacífico

Forbes (2024). Visa Peru: más del 90% de los pagos presenciales con sus tarjetas ya es contacless

IBM (S/P). ¿Qué es un ataque Mitm? (man-in-the-middle). https://www.ibm.com/think/topics/man-in-the-middle

Instituto Nacional de Defensa de la Competencia y la Propiedad Intelectual (2023). Denuncias en materia de consumo.

https://consumidor.indecopi.gob.pe/tablerosbi/#/competencias/1

Instituto Nacional de Defensa de la Competencia y la Propiedad Intelectual (2024). Resolución N° 0283-2024/SPC-INDECOPI

Instituto Nacional de Defensa de la Competencia y la Propiedad Intelectual (2024). Resolución N° 0107-2024/SPC-INDECOPI

Instituto Nacional de Defensa de la Competencia y la Propiedad Intelectual (2024). Resolución N° 0003-2024/SPC-INDECOPI

Instituto Nacional de Defensa de la Competencia y la Propiedad Intelectual (2024). Resolución N° 0102-2024/SPC-INDECOPI

Instituto Nacional de Defensa de la Competencia y la Propiedad Intelectual (2024). Resolución N° 0338-2024/SPC-INDECOPI

Pardo, J. E. (2021). La regulación de riesgos: gestionar la incertidumbre. *El Cronista del Estado Social y Democrático de Derecho*, (96), 32-45.

Quinteros, Javier (2018). *Protección al consumidor del sistema financiero: avances y retos.* Temas de Protección al Consumidor y Regulación Financiera. Círculo de Derecho Administrativo: Lima, 2018.

Reglamento de Tarjetas de Crédito y Débito, aprobado mediante la Resolución SBS N° 6523-2013

Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado mediante la Resolución SBS N° 504-2021

Reglamento de la Gestión de Conducta de Mercado del Sistema Financiero, aprobado mediante la Resolución SBS N° 3274-2017

SBS (2021). Seguridad de la información y ciberseguridad: fortaleciendo los procesos de autenticación en beneficio de los usuarios de los sistemas supervisados. *Boletín SBS, mayo 2021.*

https://acortar.link/yfobKI

SBS (2022). Autenticación reforzada: mayor seguridad para operaciones que puedan generar perjuicio al usuario. *Boletín SBS, julio 2021.*

https://acortar.link/DIEC30

SBS (2022). Entidades que provean operaciones en canales digitales deben reforzar la autenticación del usuario. *Boletín SBS, julio 2022.*

https://www.sbs.gob.pe/noticia/detallenoticia/idnoticia/2615

SBS (2024). Oficio Nº 01690-2024-SBS. Fecha: el 11 de enero de 2024