



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América
Facultad de Derecho y Ciencia Política
Escuela Profesional de Derecho

Análisis de la aplicación de las disposiciones sobre ciberseguridad en las operaciones financieras a través de canales digitales: A propósito de los recientes cambios normativos para su aplicación

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Abogada

AUTOR

Abigail Alexandra VARGAS AMARO

ASESOR

Mg. Andrés Vicente VARGAS APOLINARIO

Lima, Perú

2025



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Vargas, A. (2025). *Análisis de la aplicación de las disposiciones sobre ciberseguridad en las operaciones financieras a través de canales digitales: A propósito de los recientes cambios normativos para su aplicación*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Derecho y Ciencia Política, Escuela Profesional de Derecho]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios: Abigail Vargas / Andres Vargas

Datos de autor	
Nombres y apellidos	Abigail Alexandra Vargas Amaro
Tipo de documento de identidad	DNI
Número de documento de identidad	73475786
URL de ORCID	https://orcid.org/0009-0008-3127-1520
Datos de asesor	
Nombres y apellidos	Andres Vicente Vargas Apolinario
Tipo de documento de identidad	DNI
Número de documento de identidad	09979239
URL de ORCID	https://orcid.org/0000-0003-4521-5091
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Teresa de Jesús Seijas Rengifo
Tipo de documento	DNI
Número de documento de identidad	07957918
Miembro del jurado 1	
Nombres y apellidos	Napoleón Cabrejo Ormachea
Tipo de documento	DNI
Número de documento de identidad	05416464
Miembro del jurado 2	
Nombres y apellidos	Julio Hernán Figueroa Bustamante
Tipo de documento	DNI
Número de documento de identidad	08248540

Miembro del jurado 3	
Nombres y apellidos	Pedro Enrique Bernui Ore
Tipo de documento	DNI
Número de documento de identidad	08204622
Datos de investigación	
Línea de investigación	Derecho
Grupo de investigación	No aplica
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Metropolitana Distrito: San Isidro Latitud: -12.056445 Longitud: -77.085994
Año o rango de años en que se realizó la investigación	2024
URL de disciplinas OCDE	Derecho https://purl.org/pe-repo/ocde/ford#5.05.01



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE DERECHO Y CIENCIA POLÍTICA.

ACTA DE EXAMEN ORAL PRESENCIAL PARA EL OTORGAMIENTO DEL TÍTULO PROFESIONAL DE
ABOGADA CON TRABAJO DE SUFICIENCIA PROFESIONAL

N°072

Reunido el Jurado Examinador, constituido por los señores profesores:

- 1.-PRESIDENTA: Dra. TERESA DE JESÚS SEIJAS RENGIFO
- 2.- Dr. NAPOLEÓN CABREJO ORMACHEA
- 3.- Mg. JULIO HERNÁN FIGUEROA BUSTAMANTE
- 4.- Abg. PEDRO ENRIQUE BERNUI ORE
- 5.- Mg. ANDRÉS VICENTE VARGAS APOLINARIO (Docente Supervisor)

La bachiller postulante al Título Profesional de Abogada, doña:

ABIGAIL ALEXANDRA VARGAS AMARO

Procedió la sustentación de su Trabajo de Suficiencia Profesional, Titulado:

Análisis de la aplicación de las disposiciones sobre ciberseguridad en las operaciones financieras a través de canales digitales: A propósito de los recientes cambios normativos para su aplicación.

En la redacción del examen escrito, la graduanda fue aprobada con la nota de:

DIECISEIS (16)

Concluida la prueba oral, se practicó la votación correspondiente, resultando la candidata:

Aprobada por unanimidad con la nota doce (12)

Y para constancia se le extiende la presente acta, en Lima a los DOCE días del mes de DICIEMBRE del año 2025

Presidenta del Jurado
Dra. TERESA DE JESÚS SEIJAS RENGIFO

Dr. NAPOLEÓN CABREJO ORMACHEA

Abg. PEDRO ENRIQUE BERNUI ORE

Mg. JULIO HERNÁN FIGUEROA BUSTAMANTE

Mg. ANDRÉS VICENTE VARGAS APOLINARIO
(Docente Supervisor)



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. DECANA DE AMÉRICA
FACULTAD DE DERECHO Y CIENCIA POLÍTICA

CERTIFICADO DE SIMILITUD

Yo, Andrés Vicente Vargas Apolinario, en mi condición de docente supervisor acreditado con el Dictamen N° 000150-2025-EPD-FDCP/UNMSM, del Trabajo de Suficiencia Profesional, cuyo título es **Análisis de la aplicación de las disposiciones sobre ciberseguridad en las operaciones financieras a través de canales digitales: A propósito de los recientes cambios normativos para su aplicación**, presentado por la bachiller **Abigail Alexandra Vargas Amaro**, para optar el Título Profesional de Abogada.

CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el 8% de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional**.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para obtención del Título Profesional.

Lima, 30 de octubre de 2025

Firma del Asesor: _____

Nombres y apellidos del asesor: Andrés Vicente Vargas Apolinario

DNI: 09979239

La vigencia del presente certificado corresponde a un período de noventa (90) días desde la fecha de su emisión; siempre que no haya observaciones en el texto durante el proceso de revisión por el jurado informante o surja alguna contingencia.

Resumen:

El presente trabajo tiene como finalidad realizar un análisis exhaustivo de la normativa aplicable a las operaciones realizadas por usuarios o consumidores a través de cajeros automáticos (ATM), terminales de punto de venta (POS) y comercios electrónicos. A través de este análisis, se busca comprender las implicancias legales y regulatorias que surgen en relación con los consumos no reconocidos por los usuarios durante dichas transacciones.

El propósito es examinar la discrepancia de opiniones existente entre dos organismos reguladores clave, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (en adelante, Indecopi), con sus dos instancias, y la Superintendencia de Banca y Seguros (en adelante SBS), la cual se refleja en sus distintas resoluciones, oficios y pronunciamientos. Esta diferencia de enfoques regulatorios genera un impacto significativo en la dinámica de resolución de controversias legales, así como en la correcta implementación y cumplimiento de las normativas en el sector financiero.

Finalmente, se plantea una propuesta de solución al problema identificado, con el fin de promover una mayor claridad normativa y una mejora en la eficiencia en la resolución de conflictos dentro de este ámbito, buscando así fortalecer la confianza en los canales digitales y mejorar el marco regulatorio existente.

Palabras Clave:

Ciberseguridad, Regulación financiera, Consumos no reconocidos, Canales digitales, Controversias legales.

ÍNDICE

1. Introducción	4
2. Información del Lugar donde se desarrolló la actividad	4
2.1. Institución	4
2.2. Periodo de duración de la actividad	5
2.3. Finalidad y objetivos del centro laboral donde se desarrolló la actividad	5
2.4. Razón social	5
2.5. Dirección Postal	5
2.6. Correo Electrónico del Profesional a Cargo	5
3. Descripción de la actividad	6
3.1. Organización de la actividad (profesional a cargo)	6
3.2. Finalidad y objetivos de la actividad	6
3.3. Problemática jurídica	6
3.4. Metodología y Procedimientos	16
A) Resolución N° 0201-2024/SPC: Interpretación restrictiva del concepto de canal digital	16
B) Resolución N° 0883-2024/CC1: Ampliación del concepto de canal digital	17
3.5. Resultados de la actividad	18
3.5.1. Discusiones	18
4. Conclusiones	21
5. Recomendaciones	21
6. Bibliografía	22

1. Glosario de Términos

- **ATM:** Cajeros Automáticos (Automated Teller Machines)
- **BBVA Perú:** Banco BBVA Perú
- **CC1:** Comisión de Protección al Consumidor N° 1
- **DNI:** Documento Nacional de Identidad
- **ESF:** Entidades del Sistema Financiero
- **Indecopi:** Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual
- **LPAG:** Ley del Procedimiento Administrativo General
- **OTP SMS:** One Time Password SMS (Contraseña de un solo uso por SMS)
- **PCI DSS:** Payment Card Industry Data Security Standard
- **POS:** Terminales de Punto de Venta (Point of Sale)
- **PSP:** Proveedores de Servicios de Pago
- **RGSIC:** Reglamento de Gestión de la Seguridad de la Información y la Ciberseguridad
- **RGCM:** Reglamento de Gestión de Conducta de Mercado.
- **RT:** Reglamento de Tarjetas de Crédito y Débito
- **SBS:** Superintendencia de Banca y Seguros
- **SPC:** Sala de Protección y Defensa del Consumidor
- **TUO:** Texto Único Ordenado

2. Introducción

En el contexto actual de la transformación digital del sistema financiero, la seguridad de la información y la ciberseguridad han ido cobrando una gran importancia para garantizar la protección de los usuarios y la integridad de las transacciones digitales. Sin embargo, la regulación establecida en esta materia por la SBS ha generado relevantes discordancias por parte de los pronunciamientos del Indecopi.

Este trabajo analiza la aplicación de las normas sobre ciberseguridad en las operaciones financieras, especialmente en lo que respecta a los consumos no reconocidos en transacciones efectuadas mediante cajeros automáticos - Automated Teller Machines (ATM), terminales de punto de venta – Point of Sale (POS) y comercios electrónicos. La problemática surge a partir de la falta de consenso entre la Comisión de Protección al Consumidor del Indecopi (en adelante, la Comisión) en la interpretación del concepto de "canal digital" y la Sala Especializada de Protección al Consumidor (en adelante, la Sala), lo que ha llevado a la emisión de resoluciones contradictorias por parte de dicha institución y ha generado incertidumbre jurídica en la aplicación de las disposiciones normativas establecidas por la SBS.

A partir de un análisis profundo de la normativa especializada, las resoluciones del Indecopi y los pronunciamientos de la SBS, este estudio busca identificar las implicancias de estas divergencias regulatorias y su impacto en la seguridad del entorno financiero. Asimismo, se propone una solución de carácter regulatorio que permita la armonización de criterios, garantizando una aplicación uniforme y predecible del Reglamento de Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por la Resolución SBS N° 504-2021 (en adelante RGSIC) y del Reglamento de Tarjetas de Crédito y Débito, aprobado por la Resolución SBS N° 6523-2013 (en adelante, RT).

Finalmente, la investigación pretende contribuir al fortalecimiento de la confianza en los canales digitales, asegurando que las medidas de seguridad implementadas por las ESF cumplan con los estándares normativos sin generar cargas desproporcionadas ni afectar la eficiencia operativa de los servicios financieros digitales.

3. Información del Lugar donde se desarrolló la actividad

3.1. Institución

El trabajo de Suficiencia profesional que se presenta tiene lugar en la unidad de Regulación y Cumplimiento Normativo del área de Servicios Jurídicos del Banco BBVA Perú (en adelante, el Banco), el cual es una institución financiera reconocida a nivel nacional, cuya actividad principal consiste en la intermediación financiera.

En términos prácticos, la asistencia legal que brinda la unidad de regulación y Cumplimiento Normativo del Banco comprende lo siguiente:

- La función de Cumplimiento Normativo, la cual deriva de una obligación legal emitida por la SBS, mediante el Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado por la Resolución SBS N° 272-2017. Esta función nace de la necesidad de asegurar el estricto sometimiento y correcta adecuación de los procesos del Banco a lo establecido en la normativa externa e interna vinculada a la misma, mitigando y/o eliminando el Riesgo de Cumplimiento.
- Asesoría regulatoria, la cual se proporciona a través de un soporte integral en regulación bancaria y financiera al Banco. Entre las principales áreas con las que se mantiene comunicación permanente y brinda el servicio integral de asesoría son: Finanzas, Contabilidad, Riesgos, Compliance, Negocios, etc.
- Revisión permanente de Proyectos Regulatorios que podrían impactar a la empresa, elaborando informes, difundiendo y anticipando los cambios en nuestros procesos, asegurando que los eventuales cambios en el ambiente normativo no impacten en los negocios del Banco ni en su sometimiento estricto a las normas vigentes.
- Participación activa de principio a fin en Proyectos de Innovación de gran envergadura para el Banco, asegurando que los mismos se ajusten y cumplan con la regulación vigente, garantizando que las negociaciones y condiciones contractuales sean las más idóneas.
- Capacitación continua a los colaboradores del Banco, la cual es una función que también deriva de la Resolución SBS N° 272-2017 y tiene por objetivo asegurar que toda la organización se sensibilice y se comprometa con la Cultura de Cumplimiento Normativo.

Como parte del desarrollo de estas actividades, se ha identificado la problemática derivada del seguimiento al cumplimiento de la Regulación asociada a la Ciberseguridad dentro del sistema financiero y, en particular para las operaciones no reconocidas por los usuarios.

3.2. Periodo de duración de la actividad

Enero 2024 - diciembre 2024

3.3. Finalidad y objetivos del centro laboral donde se desarrolló la actividad

Brindar soluciones financieras integrales tanto a personas como a empresas, con el objetivo de contribuir al desarrollo económico del país.

3.4. Razón social

Banco BBVA Perú

3.5. Dirección Postal

Av. República De Panamá 3055

3.6. Correo Electrónico del Profesional a Cargo

thaissa.mirandasousa@bbva.com

4. Descripción de la actividad

4.1. Organización de la actividad (profesional a cargo)

Dentro de la unidad de Regulación y Cumplimiento Normativo mis principales funciones son la revisión diaria de incorporaciones o cambios normativos, así como de proyectos normativos con impacto en el sector financiero; elaboración de informes legales o cuadros comparativos relacionados a la normativa aplicable al Banco; seguimiento continuo del estado de adecuación de las obligaciones de carácter normativo dentro de los procesos internos del Banco en sus distintas áreas y unidades; seguimiento de precisiones o requerimientos particulares solicitados por la SBS; sostenimiento de reuniones de coordinación y entendimiento con los equipos involucrados para la implementación de una norma; asesoramiento continuo a las áreas con relación a la regulación bancaria, así como absolución de consultas legales por parte de estas, elaboración y llenado de matrices de seguimiento.

4.2. Finalidad y objetivos de la actividad

Asesoría regulatoria continua y seguimiento constante, con el propósito de asegurar el funcionamiento del negocio del Banco sin problemas legales.

4.3. Problemática jurídica

4.3.1. Realidad Problemática

La problemática de las operaciones no reconocidas realizadas en establecimientos físicos (POS, ATM) o comercios electrónicos y el cumplimiento de la regulación está relacionada principalmente con la seguridad en las mismas.

Lo antes mencionado, involucra una interacción compleja entre las prácticas comerciales, las medidas de seguridad implementadas por las ESF y las disposiciones indicadas por las autoridades regulatorias (SBS), así como la educación de los consumidores. A medida que las tecnologías avanzan, también lo hacen las técnicas de fraude, lo que obliga a los comercios y las autoridades

regulatorias a adaptarse continuamente para proteger tanto a las empresas como a los consumidores

En atención a ello, la SBS publicó el RT, mediante el cual se propuso un marco normativo para las operaciones que se realicen con los mencionados instrumentos de pago y que a su vez ello permita una mejor autenticación y validación de estas.

Adicionalmente, la SBS emitió la Resolución SBS N° 504-2021, que aprueba el RGSIC. Esta normativa, que regula la ciberseguridad en las operaciones realizadas a través de canales digitales, ha generado diversas interpretaciones a lo largo de su vigencia debido a la naturaleza general de sus disposiciones.

4.3.2. Marco Teórico

4.3.2.1. Canal Digital

Según el RGSIC (2021), *“un Canal Digital es todo medio empleado por las empresas para proveer servicios cuyo almacenamiento, procesamiento y transmisión se realiza mediante la representación de datos en bits”*.

Las disposiciones anteriores a esta norma, específicamente la Circular N° G-140-2009, abordaban la Gestión de la Seguridad de la Información. En ese documento, se hacía referencia al "canal electrónico" para las operaciones de transferencia de fondos, pero sin establecer una definición.

4.3.2.2. Sistema de Medios de Pago

- **El Consumidor y el Banco Emisor**

El **Banco Emisor** es la persona jurídica que establece un contrato con una marca de tarjeta para crear y distribuir tarjetas de crédito o débito a sus clientes (**Consumidores**). Su función en la cadena de pago se centra en:

Emisión y Gestión de Cuentas: Proporcionar los medios de pago y gestionar las cuentas de los titulares.

Autorización de Fondos: Es el Emisor quien, en última instancia, aprueba o deniega la solicitud de la transacción, verificando si el consumidor tiene saldo o crédito disponible y aplicando sus propios mecanismos antifraude internos basados en el perfil del cliente.

- **La Adquirencia: Bancos Adquirentes y Operadores Tecnológicos**

La adquirencia se define como la capacidad de un establecimiento comercial para aceptar pagos con tarjeta. Este proceso es gestionado por el adquirente, cuya función se divide entre el riesgo financiero y la operación tecnológica:

Banco Adquirente (Función Regulatoria y Financiera): Es la entidad financiera supervisada (banco o similar) que **asume la responsabilidad legal y financiera** frente al Banco Emisor y a las Marcas de Tarjetas por las transacciones del comercio que afilian. Su rol es importante en la liquidación

de fondos y en la **asunción inicial del riesgo** por contracargos (*chargebacks*).

Operadores y Proveedores de Servicios de Pago (PSPs): Entidades como **Niubiz, Izipay o Qulqi** son los operadores tecnológicos que proveen la infraestructura. Ellos:

- **Establecen el Acuerdo con el Comercio:** Firman el contrato comercial para aceptar tarjetas.
- **Proveen Tecnología:** Suministran los terminales **POS** y las **Pasarelas de Pago** (el *software* de conexión para el comercio electrónico).
- **Procesamiento Operativo:** Capturan, cifran y envían la solicitud de pago para su autorización.

La seguridad operativa en el punto de venta o en el comercio electrónico es responsabilidad directa del Adquirente y de sus operadores, quienes están obligados a cumplir con estándares industriales (como PCI DSS).

- **Pasarelas de Pago y Marcas de Tarjetas**

Estos actores actúan como intermediarios tecnológicos y normativos:

Marcas de Tarjetas (Redes de Procesamiento): Entidades como **Visa o Mastercard** son redes globales que operan la infraestructura para mover la información y el dinero entre el Emisor y el Adquirente. Su rol no es emitir, sino **establecer las reglas del juego**, definir los **estándares de seguridad** (ej., PCI DSS) y gestionar la tecnología de autenticación avanzada para compras en línea (ej., 3D Secure).

Pasarelas de Pago: Es el servicio o *software* que actúa como el enlace de seguridad entre el sitio web del comercio y el procesador del Adquirente. Su función primordial es obtener los datos sobre la tarjeta de forma segura, cifrarlos y actuar como un filtro de validación preliminar antes de enviar la solicitud a la ESF.

- **Uso de cajeros Automáticos (ATM)**

De acuerdo al Reglamento de Canales Complementarios, aprobado por la Resolución SBS N° 4798-2015, los cajeros automáticos son dispositivos electrónicos interconectados que permiten a las ESF ofrecer diversas operaciones y servicios a los usuarios. Esto se logra a través del uso de tarjetas, u otros métodos de identificación que impliquen firmas electrónicas o similares, siguiendo un procedimiento definido por la empresa, el cual es comunicado y aceptado por el cliente.

4.3.2.3. Medidas de seguridad en establecimientos

El RT establece que las ESF deben adoptar medidas de seguridad idóneas con la finalidad de verificar la autenticidad del uso de las tarjetas y asegurar el cumplimiento de las condiciones correspondientes.

En este contexto, de acuerdo al artículo 18 del citado reglamento al formalizar acuerdos con operadores o establecimientos, los bancos deben garantizar que estos asuman, cuando corresponda, las siguientes responsabilidades:

- Implementar procedimientos para aceptar operaciones, que incluyan, entre otros, la validación de la tarjeta y la identificación del usuario.
- No almacenar ni retener la información de las tarjetas en bases de datos, ya sean manuales o digitales, excepto cuando sea necesario para autorizar una transacción.
- Cumplir con los requerimientos en lo relacionado a seguridad establecidos en el Reglamento, según corresponda.

4.3.2.4. Operaciones no Reconocidas por los usuarios

Adicionalmente a lo indicado líneas arriba, el RT también dispone que si una transacción es rechazada o un usuario reclama que fue ejecutada de manera incorrecta, la empresa tiene la responsabilidad de llevar a cabo la evaluación pertinente y evidenciar que las operaciones pasaron por la debida autorización y registro.

4.3.2.5. Proceso de Autenticación de los usuarios

- **Factores de Autenticación**

El RGSIC (2021) dispone que los factores de autenticación son aquellos mecanismos utilizados para validar la identidad del usuario y tienen las siguientes categorías:

- Algo que solo el usuario conoce (por ejemplo una contraseña).
- Algo que solo el usuario posee (por ejemplo su celular, DNI, entre otros).
- Algo que el usuario es, que incluye las características biométricas (por ejemplo la huella dactilar, factores biométricos).

- **Enrolamiento a un Canal Digital**

De acuerdo al RGSIC (2021), el enrolamiento de un usuario en un canal digital requiere por lo menos:

- a) Verificar la identidad del usuario y tomar las medidas necesarias para reducir la posibilidad de suplantación de identidad, lo que incluye el uso de dos factores de autenticación de categorías diferentes e independientes.
- b) La generación de credenciales y asignación al usuario

Finalmente es responsabilidad de las ESF gestionar el ciclo de vida de las credenciales que dicha empresa genera y asignarlas a los usuarios.

- **Autenticación Reforzada**

El RGSIC establece que se debe efectuar un procedimiento de autenticación reforzada en aquellas actividades que puedan dar lugar a operaciones

fraudulentas o abusos que perjudiquen al cliente. Esto abarca transacciones realizadas a través de canales digitales que impliquen pagos o transferencias de fondos a personas distintas al usuario, el registro de beneficiarios de confianza, modificaciones en productos como seguros, ahorro o inversión, la contratación de nuevos productos o servicios, así como ajustes en los límites y condiciones.

Para ello, se requiere:

- Usar dos factores de autenticación, los cuales deben ser de categorías distintas e independientes entre sí.
- Aplicar mecanismos de protección contra ataques de tipo "hombre en el medio", como la generación de un código único basado en los datos específicos de cada transacción, el cual debe ser de uso único.
- En caso de que la operación sea exitosa, enviar una notificación al usuario con los detalles correspondientes.

4.3.3. Antecedentes

4.3.3.1. Reglamento para la Seguridad de la Información y Ciberseguridad (Resolución SBS N° 504-2021)

La SBS aprobó el RGSIC el 19 de febrero de 2021 cuyo objetivo era garantizar que las ESF operen en entornos seguros y confiables al ofrecer sus productos y servicios, anticipando los riesgos derivados del avance tecnológico, la interconectividad y la transformación digital.

El reglamento asigna responsabilidades específicas a distintas unidades y áreas de las ESF, tales como las unidades relacionadas con la operatividad y sistemas.

El reglamento también establece requisitos para la autenticación en canales digitales, incluyendo la implementación de autenticación reforzada en operaciones de riesgo, así como su enrolamiento previo para el ingreso a un entorno seguro.

La norma entró en vigencia el 1 de julio de 2021, excepto para los requisitos de autenticación, que comenzaron a aplicarse el 1 de julio de 2022.

Tras la entrada en vigencia de la norma mencionada, el Banco fortaleció sus controles de seguridad en las operaciones realizadas a través de canales digitales tales como su Banca móvil, Banca por internet y la zona pública.

Ahora bien, el concepto de "canal digital" definido en la norma se basa en el uso de dispositivos electrónicos que operan mediante "bits", dicha acepción, es amplia, ya que implica que cualquier tecnología digital que permita la interacción, comunicación o procesamiento de datos podría entrar en esta categoría. Esta interpretación podría sugerir que aquellos canales que actualmente son considerados presenciales, así como aquellos en los que no se necesita un proceso de enrolamiento anterior sean considerados canales digitales, ya que su naturaleza electrónica y la capacidad de transmitir o

procesar información de manera digital son los elementos clave para su clasificación.

Bajo esta premisa, diversos puntos de interacción con los usuarios pueden ser considerados canales digitales, aunque por su forma de reconocimiento y relación no se los reconozca como tales. Entre ellos se encuentran:

- Cajeros automáticos (ATM): Estos dispositivos permiten operaciones financieras automatizadas mediante interfaces electrónicas, accediendo a redes digitales para la validación de transacciones.
- Puntos de Venta (POS) en comercios físicos: Aunque se ubican en entornos presenciales, los POS operan dentro de un ecosistema digital que involucra la validación en línea de pagos, la autenticación del usuario y la conexión con redes financieras.
- Comercios electrónicos: Espacios en línea donde los usuarios realizan transacciones digitales a través de plataformas de pago que cumplen funciones de autenticación y validación de operaciones.

Esta interpretación más amplia del término “canal digital” resalta la importancia de aplicar medidas de seguridad y autenticación sólidas en todos los entornos donde se procesen transacciones digitales. Esto implica que dichas medidas no deben limitarse únicamente a plataformas en línea o dispositivos previamente registrados, sino que también deben contemplar otros puntos de interacción donde se realicen operaciones electrónicas. No obstante, la normativa vigente no especificaba con claridad sobre el uso de estas medidas.

En base a lo indicado, el Banco optó por clasificar las operaciones con tarjetas; siendo que en algunos casos se requiere un enrolamiento previo para efectuar la transacción y aquellas donde no es viable realizar esto o también se requiere la presencialidad del usuario (operaciones en cajeros, ATM, comercios electrónicos). Bajo esta categorización, no se consideraba necesario implementar la totalidad de las disposiciones relacionadas con la autenticación de los usuarios que sí se exigen en entornos digitales.

Esta interpretación se sustentaba en el hecho de que el tratamiento de dichas operaciones ya estaba regulado en el RT y precisado en los Oficios N° 26791-2017 y N° 1793-2019, los cuales hacen referencia al Reglamento de Gestión de Conducta de Mercado (en adelante, RGCM) indicando que, en la ejecución de un contrato de producto financiero (como en el caso de operaciones que impliquen el uso de una línea de crédito) las empresas están obligadas a validar la identidad del cliente y a registrar evidencia de la aceptación del mismo. Para ello, se permite el uso de diversos mecanismos de autenticación.

Asimismo, se establece que para poder asumir el monto de una operación realizada con una tarjeta de crédito con cargo a la línea que ha sido otorgada al titular, la entidad emisora debe contar con órdenes de pago que se encuentren suscritas o autorizadas por el cliente. En el caso de transacciones presenciales en establecimientos, el POS generalmente emite un voucher con la firma del cliente, además de indicar el número de su DNI, excepto cuando sea un micropago. Por lo tanto, para defenderse ante un reclamo, la ESF debía

presentar el voucher firmado por el cliente para justificar el cargo, o, si se trata de un micropago, demostrar la responsabilidad del usuario.

Adicionalmente, el RT preveía en su artículo 12 que *“para el uso de operaciones con tarjetas de débito se debía solicitar una clave secreta, firma, firma electrónica u otros mecanismos que permitan identificar al usuario, de acuerdo con lo pactado”*.

Lo anterior confirma que la versión inicial de la norma presentaba falta de claridad, ya que existían regulaciones emitidas por la SBS que no eran totalmente compatibles con el RGSIC. Esto resultaba especialmente relevante dado que las operaciones en cuestión se realizaban en un entorno predominantemente presencial o no requerían algún enrolamiento previo.

La problemática central radica en la inicial falta de claridad de la normativa, un hecho confirmado por las inconsistencias detectadas. Específicamente, existían regulaciones emitidas por la SBS que no lograban una compatibilidad total con lo estipulado en el RGSIC. Esta situación adquiría una relevancia particular al considerar que las operaciones en cuestión se desenvolvían predominantemente en un entorno físico o presencial. Además, una característica distintiva de estas transacciones era que no demandaban un enrolamiento previo por parte de los usuarios, lo que acentuaba la disparidad. Como resultado directo de estas incongruencias, se generaban discrepancias significativas en la aplicación de las medidas de autenticación que eran exigidas para las transacciones realizadas en el ámbito digital, creando un vacío y una dificultad en la homologación de los procedimientos de seguridad entre ambos entornos operativos.

4.3.3.2. Boletines Normativos

En varias ediciones de los boletines emitidos por la SBS se pronunciaron sobre el RGSIC. Para el tema que nos ocupa destacamos el Boletín y su nota de prensa de julio 2022, mediante el cual la SBS indicó que los POS, ATM y comercios electrónicos eran considerados canales digitales; sin embargo, como lo indicaremos más adelante la propia SBS indicó que este tipo de publicaciones no tenían carácter regulatorio.

4.3.3.3. Instrucciones sobre aplicación de la Resolución SBS N° 504-2022

Oficio N° 36482-2022 - Precisiones sobre Factores

El 31 de agosto del 2022, mediante el Oficio de referencia la SBS estableció diversas precisiones con relación al uso de los factores de autenticación en las operaciones en canales digitales que requieren autenticación reforzada.

- **Preguntas reto:** Su uso como factor que conoce solo el usuario, para fines de autenticación reforzada, requiere que sea el usuario quien las establezca además de que cuando se almacena o transfiere sea de forma cifrada.
- **Uso del OTP SMS:**

- *Uso para el enrolamiento:* Su uso como factor de autenticación para probar su posesión mediante el envío de una OTP vía SMS al teléfono móvil, no es válido debido a su vulnerabilidad al SIM swapping.¹
- *Uso para la autenticación reforzada:* Si su uso se realiza con una aplicación móvil instalada, como factor que solo posee el usuario, cuya posesión es probada mediante el uso de una OTP recibida en dicha aplicación móvil, no constituye un factor válido, a menos que dicho uso esté condicionado a que la aplicación verifique que el dispositivo móvil corresponde a aquel afiliado por el usuario al momento del enrolamiento.
- **Firma manuscrita:**
 - *Registro mediante un voucher o a través de una pantalla táctil:* No se considera un factor de autenticación inherente, a menos que exista una validación de dicho factor que sea inmune a las amenazas de suplantación, tenga una alta tasa de éxito y se pueda contrastar con un registro oficial o previamente establecido por la empresa.
 - *Uso en medios de pago:* La autenticación es un proceso para verificar que el usuario es quien dice ser, para lo cual se contrastan factores de las tres categorías mencionadas previamente. En dicho contexto, registrar una firma manuscrita en medios de pago o en una pantalla táctil no constituye una validación biométrica.
- **Biometría (huella digital o reconocimiento facial):** el uso por medio de dispositivos móviles u otros no constituye un factor de autenticación inherente, con excepción de que la validación pueda resistir a amenazas de suplantación, con una gran alta probabilidad de éxito (minimizar falsos positivos y falsos negativos), el cual puede ser contrastado con un registro oficial o previamente constituido por la empresa.
- **Tarjeta:** La posesión de una tarjeta de crédito o débito, así como la información contenida en ellas, como factor que solo posee el usuario, constituye un único factor de autenticación, el cual debe ser complementado con otro factor para que resulte aplicable como parte de la autenticación reforzada.
- **Documento nacional de identidad (DNI):** El número de DNI no constituye un factor de autenticación permitido para confirmar la identidad del usuario; y, en el caso donde se utilice el reconocimiento estructural del DNI, la ESF debe contar con evidencia de la razonabilidad de su uso y de una alta probabilidad de éxito al momento de la autenticación.

A partir de lo expuesto anteriormente, podría interpretarse que las operaciones con tarjetas realizadas de manera presencial también estarían comprendidas dentro del ámbito de aplicación del RGSIC, ya que se indican mecanismos relacionados con la firma manuscrita y el uso de una tarjeta. No obstante, es importante aclarar que el referido oficio no modificó la aplicación

¹ El SIM Swapping es un tipo de robo de identidad en el que los delincuentes obtienen el control del número de móvil de una víctima, generalmente haciéndose pasar por ellos ante su operador. Esto permite a los estafadores acceder a llamadas, mensajes de texto y datos, lo que lleva a robos financieros, robos de identidad adicionales y pérdida de acceso a cuentas. Para evitarlo, las personas deben usar contraseñas seguras, aplicaciones de autenticación en lugar de SMS para la autenticación de dos factores, establecer un PIN de operador fuerte, tener cuidado con el phishing y monitorear la actividad de la cuenta. Si se sospecha de un intercambio de SIM, los pasos inmediatos incluyen ponerse en contacto con el operador de telefonía móvil, los bancos y la policía, cambiar contraseñas y monitorear el crédito. y la ausencia de condiciones técnicas que aseguren la confidencialidad de la transmisión de los mensajes SMS.

del RT o del RGCM (donde aún se mencionaba la aplicación de firmas manuscritas como factor de autenticación), ello en atención al principio de jerarquía normativa y especialidad normativa.

En este sentido, el cumplimiento de las medidas de seguridad y las disposiciones referidas a la autenticación debió basarse en la normativa específica que regula estas operaciones. Adoptar una postura contraria generaría inconsistencias jurídicas y una interpretación poco coherente con la naturaleza de las transacciones en entornos presenciales o aquellas que no requieren un enrolamiento previo, lo que podría afectar su adecuado tratamiento normativo y operativo; como lo vemos a continuación.

Oficio N° 01690-2024 - Precisiones sobre el RGSIC

El 11 de enero del 2024, la SBS difundió un oficio múltiple (indicado en la referencia), mediante el cual absuelve las consultas realizadas por el Indecopi con relación a la interpretación de las disposiciones del RGSIC.

Al respecto, toma en cuenta la definición establecida preliminarmente por el RGSIC, por tanto como únicamente se requiere que su representación se de a través de bits, todos aquellos canales que cumplan con dicha definición, a través de los cuales las ESF proveen sus servicios a los usuarios, son considerados canales digitales, en lo que concierne a dichos servicios.

Las ESF deben verificar la identidad del usuario para transacciones que lo requieran, como el pago de servicios, tanto en sus propios canales como en los de terceros.

Tomando en consideración la interpretación realizada por la SBS, las precisiones efectuadas hacen referencia a las operaciones efectuadas con POS en tarjetas de crédito, lo que indicaría que la aplicación del RGSIC también abarcaría este tipo de transacciones, independientemente de que las mismas no requieran un enrolamiento previo o se realicen en un entorno presencial.

No obstante, cabe destacar que esta precisión fue establecida con posterioridad a la entrada en vigencia de la norma, lo que generó un período de incertidumbre respecto a su aplicación. Durante ese lapso de tiempo, el Banco adoptó una postura distinta, basada en la regulación previa y en la interpretación original del alcance normativo. Dicha postura fue tomada en cuenta y adoptada por la Sala de protección de defensa y protección al consumidor del Indecopi para casos de operaciones realizadas con tarjetas emitidas por el Banco y que fueron utilizadas cuando no se requirió un enrolamiento previo del usuario, las cuales serán analizadas a continuación.

Resoluciones contrapuestas emitidas por el Indecopi

Resolución N° 0201-2024/SPC de fecha 24 de enero de 2024 (Señor Montilla vs. BBVA Perú)

El señor Jimmy Arnold Montilla Huamán denunció que el 18 de julio de 2022, aproximadamente a las 17:07 horas, se realizaron tres transacciones que él no reconocía:

- Una desde su cuenta de ahorros por S/ 6 500,00.
- Dos pagos realizados con cargo a su tarjeta de crédito N° 4147-\\-\\-\\-0901 por US\$ 3 000,00 y US\$ 700,00.

El señor Montilla indicó que en la fecha de los hechos, aproximadamente a las 16:44 horas, se quedó sin señal en su teléfono móvil y, al intentar ingresar a su aplicativo del Banco, se percató de que su contraseña había sido cambiada.

Al respecto, en su respuesta el Banco negó su responsabilidad por las operaciones, argumentando que se realizaron con los datos sensibles de la tarjeta activa del cliente y que estaban dentro de su patrón habitual de consumo.

Sobre el caso, la Sala indicó los siguientes puntos en lo referido a la aplicación del RGSIC:

- **El Enrolamiento como Punto de Partida:** La Sala dictaminó que un medio electrónico sólo califica como "canal digital" bajo la normativa de ciberseguridad si el usuario ha completado un proceso previo de enrolamiento. Este proceso implica la validación de la identidad y la creación de credenciales de acceso para operar en dicho canal.
- **Identificación de Canales "Digitales":** Según este requisito de enrolamiento, la Sala clasificó como "canales digitales" a aquellos que exigen autenticación previa (eso es, un enrolamiento), tales como la banca móvil de la ESF, la banca por internet, las billeteras digitales y plataformas parecidas que demandan un registro previo (ej., Net Cash, Multired celular).
- **Medios no Considerados "Digitales":** En contraste, se determinó que dispositivos como cajeros automáticos (ATM), puntos de venta (POS), plataformas de comercio electrónico y ventanillas de atención al público no se rigen por esta definición de "canal digital" en el marco del RGSIC, ya que no requieren un enrolamiento previo del usuario.
- **Alcance Específico de la Autenticación Reforzada:** El artículo 19° del RGSIC enumera detalladamente las operaciones que exigen una autenticación reforzada, tales como transferencias o pagos a terceros, la adición de beneficiarios de confianza o la contratación de nuevos servicios. Esto aclara que no todas las transacciones están sujetas a este nivel de seguridad.
- **Naturaleza No Regulatoria de los Boletines de la SBS:** La Sala subrayó que los boletines informativos de la SBS son meramente informativos y no poseen carácter normativo. Por lo tanto, no pueden utilizarse para extender la interpretación de la regulación más allá de lo explícitamente contenido en ella.

Las operaciones impugnadas se efectuaron mediante una plataforma de comercio electrónico, por tanto dado que estas plataformas no demandan un enrolamiento previo del usuario según la interpretación de la Sala, **se dictaminó que el RGSIC no aplicaba a esta situación.**

Por ende, la evaluación de la responsabilidad del proveedor (Banco BBVA Perú) se llevó a cabo de acuerdo a lo establecido en el RT y el Código de Protección al Consumidor. La decisión final revocó la resolución anterior, mediante la cual se había declarado fundada la denuncia contra el Banco, declarándola ahora infundada. La Sala consideró que las operaciones se ajustaban a los consumos habituales del cliente y se ejecutaron cumpliendo los requisitos de validación exigidos, haciendo hincapié en el deber de las ESF de monitorear operaciones inusuales, según el artículo 17° del RT.

Resolución N° 0883-2024/CC1 de fecha 03 de abril de 2024 (señora Chamochumbi vs. BBVA Perú)

Con fecha 03 de abril de 2024, la Comisión emitió un pronunciamiento en el que aplicó el RGSIC y las precisiones establecidas por la SBS, en contradicción con lo establecido en la resolución previa.

Las operaciones no reconocidas consistieron en un cargo de US\$ 2 390,52 en la tarjeta de crédito adicional N° 5536-****-****-8286 de la Sra. Chamochumbi, el 30 de agosto de 2023. La Sra. Chamochumbi alegó que la tarjeta pudo haber sido clonada, que el banco no la alertó sobre la operación sospechosa, y que la transacción no se realizó con su clave secreta.

El Banco respondió que la Sra. Chamochumbi solicitó la tarjeta adicional para el Sr. Christopher Tarpey Chamochumbi. Argumentó que la operación se realizó en un establecimiento comercial en Chile con la presencia de la tarjeta y la digitación de la clave secreta. Además, indicó que la tarjeta fue bloqueada después de la operación cuestionada y que no generó una alerta porque se encontraba acorde al patrón habitual de consumo de la denunciante. Finalmente, mencionó que la Sra. Chamochumbi no estaba afiliada al sistema de notificaciones.

Al respecto, según lo señalado por el Indecopi, la SBS aprobó el RGSIC, el cual establece un marco normativo de referencia para el sistema de gestión de ciberseguridad, con el propósito de fortalecer las capacidades en ese entorno y mejorar los procesos de autenticación en las ESF, garantizando así un entorno de operaciones seguro y confiable.

En este contexto, se determina que cualquier operación realizada a través de un medio que utilice datos en bits—entendiéndose los bits como la unidad mínima de información— y que involucre procesos de almacenamiento, procesamiento y transmisión de datos en formato digital, debe ser considerada como una operación realizada mediante un canal digital.

La postura que adoptó la comisión fue en base a lo establecido por la SBS en el Oficio N° 01690-2024-SBS, en el cual se establece que el canal por medio del cual la usuaria (POS) es considerado un canal digital, ya que su transferencia se permite a través de bits, por lo cual debe ser considerados como canal digital en lo que respecta a dichos servicios.

Asimismo, la SBS precisó que las acciones que puedan derivar en operaciones fraudulentas o abusos del servicio en perjuicio del cliente no se limitan únicamente a las mencionadas en el artículo 19° del RGSIC, sino que también incluyen, entre

otros, los aplicativos móviles, la banca por internet, las billeteras digitales, los cajeros automáticos (ATM), los terminales de punto de venta (POS) y las transacciones de comercio electrónico que empleen instrumentos de pago proporcionados por las ESF.

En ese sentido, el Indecopi concluyó que el Banco no adoptó las medidas de seguridad necesarias al permitir una operación no reconocida por US\$ 2 390,52 en la tarjeta de crédito adicional de la Sra. Chamochumbi.

Resolución 2650-2024/SPC-INDECOPI de fecha 23 de septiembre de 2024 (Sra. Mantilla vs. BBVA Perú)

El caso se originó con la denuncia de la señora Eliana Marliss Mantilla Benavides contra el Banco ante la Comisión. La denunciante alegó que entre el 30 de marzo y el 26 de abril de 2022, el Banco permitió la realización de 17 operaciones no reconocidas con una tarjeta de débito, por un total de S/ 16 318,59. Argumentó que estas operaciones no correspondían a su patrón de consumo, se realizaron en un corto tiempo y en el mismo establecimiento comercial (FpaySodimac y FpayHIPERMER), por lo que debieron generarse alertas. La Comisión declaró fundada la denuncia en primera instancia.

En respuesta, el Banco apeló la resolución, presentando como prueba que las compras por internet se encontraban habilitadas desde el 30 de marzo de 2022, antes de las operaciones cuestionadas. Sostuvo que las transacciones se realizaron válidamente y dentro del patrón de consumo de la clienta, acreditando el uso de datos sensibles y confidenciales de la tarjeta, así como los códigos de autorización generados que validaban la operación. El Banco argumentó que el resguardo de la clave secreta era responsabilidad de la tarjetahabiente y que había cumplido con sus medidas de seguridad.

En este caso nuevamente determinó que las operaciones cuestionadas formaban parte del comportamiento habitual de consumo de la denunciante, ya que ninguna excedía el importe máximo de S/ 45 000,00 registrado previamente. Además, concluyó que el Banco demostró que las operaciones se realizaron válidamente, con la tarjeta habilitada para compras por internet y mediante el ingreso de datos sensibles de la tarjeta. En cuanto a la aplicación del RGSIC, la Sala precisó que no era aplicable al caso porque las operaciones se realizaron en comercios electrónicos, por lo cual no debía ser considerado como canal digital al no poder efectuarse un enrolamiento previo.

Las tres resoluciones emitidas por el mismo organismo institucional, aunque abordan temáticas similares, carecen de una uniformidad preocupante en su criterio. Esta inconsistencia se manifiesta en la aplicación de enfoques dispares para situaciones que presentan similitudes inherentes, lo que genera una ambigüedad significativa en el marco regulatorio. Como resultado, tanto la interpretación como la aplicación de la normativa se ven obstaculizadas, creando un entorno de incertidumbre que repercute directamente en las ESF.

En particular, el Banco enfrenta desafíos considerables para asegurar una correcta implementación y adecuación regulatoria, viéndose expuesto a posibles riesgos de cumplimiento y operativos.

Esta falta de coherencia no solo complica el cumplimiento normativo para las ESF, sino que también puede conducir a disparidades en la supervisión y a posibles asimetrías en el mercado. La ausencia de un criterio unificado dificulta la planificación estratégica de las entidades, ya que no pueden prever con certeza cómo se interpretarán las regulaciones en el futuro. Más adelante, profundizaremos en las implicaciones detalladas de esta situación, analizando cómo afecta la operativa diaria del Banco.

4.3.4. Formulación del problema general

Problema

¿De qué manera la divergencia interpretativa de Indecopi (Sala y Comisión) y la SBS sobre el concepto de 'canal digital' y la aplicación del RGSIC a operaciones en ATM, POS y comercio electrónico incide en la seguridad jurídica y la resolución de controversias por consumos no reconocidos en el sistema financiero peruano?

Problema específico 1

¿Qué impacto tiene esta inseguridad jurídica en la implementación de medidas de ciberseguridad por parte de las ESF?

Problema específico 2

¿Cómo influye en la protección efectiva de los derechos de los consumidores?

Objetivo general

Evaluar críticamente la discrepancia interpretativa entre la Sala y la Comisión del Indecopi, así como los pronunciamientos de la SBS, en torno a la definición de 'canal digital' y la aplicabilidad del RGSIC a operaciones en ATM, POS y comercio electrónico, a fin de determinar su impacto en la seguridad jurídica y la resolución de controversias por consumos no reconocidos.

Objetivo específico 1

Analizar la justificación y las implicancias de la interpretación del Indecopi, contrastándola con la visión de la SBS.

Objetivo específico 2

Determinar el impacto de estas interpretaciones contradictorias en la determinación de la responsabilidad y aplicación normativa por parte de las ESF.

Hipótesis general

La divergencia interpretativa entre la Sala y la Comisión del Indecopi, así como los pronunciamientos de la SBS, respecto a la definición de "canal digital" en el RGSIC y su aplicación a operaciones en ATM, POS y comercio electrónico, genera inseguridad jurídica en el sistema financiero

peruano y menoscaba la eficacia en la resolución de controversias por consumos no reconocidos.

Hipótesis específica 1

La interpretación amplia del concepto de 'canal digital' por parte de la Comisión del Indecopi impone cargas y obligaciones desproporcionadas a las ESF, sin una clara justificación normativa.

Hipótesis específica 2

La falta de un criterio unificado entre Indecopi en la definición de 'canal digital' afecta la predictibilidad de las decisiones administrativas y la capacidad de las ESF para implementar estrategias de ciberseguridad efectivas.

4.4. Metodología y Procedimientos

1. Tipo de investigación

La metodología utilizada en este trabajo de investigación es de tipo descriptiva y analítica.

2. Metodología

La metodología empleada en este trabajo de suficiencia es de tipo descriptivo y analítico. Adopta un enfoque descriptivo para ofrecer una visión detallada de cómo el sector financiero cumple con el RGSIC, mientras que la perspectiva analítica permite un examen crítico de los datos recopilados, derivando en conclusiones y recomendaciones pertinentes.

3. Técnicas e instrumentos

Resoluciones emitidas por el Indecopi (Casos entre el Banco e Indecopi), oficios múltiples emitidos por la SBS y disposiciones normativas.

4. Análisis de las Resoluciones del Indecopi y Oficios de la SBS en relación a las operaciones no reconocidas por clientes del Banco.

Las resoluciones emitidas por el Indecopi presentan posturas distintas respecto a la interpretación del RGSIC y su aplicación a las operaciones realizadas a través de ciertos canales, particularmente en relación con POS, cajeros automáticos y comercios electrónicos. En ese sentido, efectuaremos un análisis de ambas.

A) Resolución N° 0201-2024/SPC

La Resolución N° 0201-2024/SPC-Indecopi estableció una postura sobre la definición de "canal digital" en el marco del RGSIC, así como de los aspectos relacionados a la normativa vigente publicada por la SBS y su coherencia con el actual ecosistema de pagos, a pesar de lo indicado en el Oficio N° 01690-2024. Tal como lo indicamos previamente, en este oficio, la SBS expone una visión más inclusiva del concepto de canal digital. La esencia de este oficio radica en que, si bien la SBS reconoce que la autenticación reforzada del RGSIC se vincula al enrolamiento, su propia concepción de "canal digital" es más vasta, abarcando

cualquier medio electrónico o remoto que posibilite la interacción con servicios financieros, independientemente de si requiere un enrolamiento directo con la entidad para una operación específica.

Más allá de la interpretación normativa, la viabilidad operativa de considerar las transacciones por POS, ATM o comercios electrónicos como "canales digitales" en el sentido que exige autenticación reforzada y enrolamiento, presenta desafíos significativos para las ESF.

Primero, la infraestructura actual de muchos comercios, especialmente los pequeños y medianos, no está diseñada para soportar los requisitos de autenticación reforzada que se aplicarían si sus puntos de venta (POS) o plataformas de comercio electrónico fueran clasificados como canales digitales bajo una interpretación estricta. Implementar esta tecnología requeriría una inversión masiva en hardware y software, además de una capacitación exhaustiva para el personal de los comercios. Esto podría ralentizar las transacciones, generar fricción para el usuario y, en última instancia, perjudicar la adopción de pagos electrónicos.

Segundo, la experiencia del usuario se vería seriamente afectada. Imaginar la necesidad de un proceso de enrolamiento o autenticación reforzada similar al de una banca móvil para cada transacción en un POS o ATM, o incluso en un comercio electrónico no bancarizado, es poco práctico. Esto iría en contra de la rapidez y la conveniencia que los usuarios esperan de estos medios de pago, generando frustración y potencialmente llevando a un retorno al uso de efectivo. La esencia de las transacciones en estos puntos es la agilidad.

Tercero, el costo de asumir esta nueva definición sería inmenso para las ESF. No solo implicaría la adaptación de sus propios sistemas y la capacitación de su personal, sino también un acompañamiento y una inversión en la infraestructura de miles de comercios asociados. Estos costos, inevitablemente, serían trasladados a los clientes finales a través de mayores comisiones o tarifas por el uso de estos servicios, lo que podría desincentivar aún más el uso de medios de pago electrónicos y afectar la inclusión financiera.

Ahora, si bien el Oficio N° 01690-2024-SBS-PRI de la SBS presenta una visión más amplia de "canal digital" en un contexto general de "medios electrónicos o remotos" para servicios financieros, la Sala tomó puntos válidos para no adoptar esta perspectiva, como lo detallamos a continuación:

- **Precisión Normativa vs. Generalidad Conceptual:** La interpretación del Indecopi se afianza en el texto y a las disposiciones del *RGS/C*, que vincula explícitamente el "canal digital" con el proceso de enrolamiento.

El Oficio de la SBS, no puede modificar o ampliar la definición específica contenida en una norma de mayor jerarquía y especificidad regulatoria. Defender la interpretación estricta de la Sala es necesario para mantener la jerarquía normativa y evitar que conceptos generales (como los del Oficio) diluyan las exigencias específicas de un reglamento de seguridad.

- **Delimitación de Responsabilidades Claras:** La Sala, al insistir en el enrolamiento, asegura que las obligaciones de ciberseguridad y la

responsabilidad asociada recaigan sobre aquellos canales donde las ESF tienen un control directo y verificable sobre la identidad y autenticación del usuario. Por tanto, extender el concepto de "canal digital" a cualquier medio remoto, sin un proceso de enrolamiento que asegure la autenticación de la entidad, podría generar una dilución de responsabilidades y expectativas de seguridad poco realistas para los proveedores.

- **Foco en la autenticación y el control directo:** La visión de la Sala se enfoca en la autenticación robusta y el control que la ESF tiene sobre el acceso al canal. Las operaciones realizadas en plataformas de comercio electrónico, aunque digitales, se rigen por la lógica de validación de la tarjeta o del medio de pago, no por un enrolamiento previo en el "canal digital" de la entidad financiera. Es decir, la seguridad recae en el sistema de pago y no en el cumplimiento de las obligaciones de enrolamiento de un "canal digital" bajo el RGSIC.

De acuerdo a lo dispuesto por e RT, la normativa obliga a las ESF a implementar rigurosas medidas en lo relacionado a las disposiciones sobre seguridad de la información para salvaguardar el ciclo de vida de los datos de las tarjetas (almacenamiento, procesamiento y transmisión). Las exigencias generales requieren que las empresas observen las normas de la Superintendencia sobre seguridad y continuidad del negocio.

Añadiendo a esto, el artículo detalla un conjunto de controles específicos que deben ser aplicados. Es mandatorio asegurar y mantener los cortafuegos y equipos de red con configuraciones estandarizadas para restringir accesos, además de proteger la información mediante la implementación de cifrado durante su transmisión en redes públicas. La integridad de los sistemas se resguarda manteniendo *software* antivirus actualizado y asegurando que las aplicaciones sean robustas contra vulnerabilidades, lo cual incluye prohibir el uso de claves secretas predeterminadas por los proveedores. El control interno y la prevención se refuerzan con la exigencia de limitar el acceso a los datos solo al personal estrictamente autorizado, asignar un identificador único a cada usuario con acceso, y realizar periódicamente análisis de vulnerabilidades y pruebas de penetración (internas y externas).

B) Resolución N° 0883-2024/CC1

La Comisión adoptó una postura que amplía el alcance del concepto de "canal digital", extendiendo la aplicación del RGSIC a un espectro más amplio de operaciones. Los puntos fuertes de esta argumentación radican en su enfoque teleológico del reglamento y su alineación con la evolución tecnológica y la propia postura de la SBS en otros documentos.

- **Priorización del Objetivo Fundamental del RGSIC:** La Comisión sustenta su decisión en una lectura que va más allá de la literalidad, centrándose en la finalidad última del RGSIC. Argumenta con convicción que la norma fue concebida para establecer un marco de seguridad de la información comprensivo, cuyo fin principal es robustecer la ciberseguridad y perfeccionar los mecanismos de autenticación en todas las ESF.

- **La Naturaleza "Digital" Intrínseca a los Datos Binarios:** Un argumento central y convincente de esta resolución radica en su afirmación de que "cualquier operación que emplee datos en bits, sin importar el medio por el cual se transmita, debe ser catalogada como una operación digital". Esta definición es notablemente más pertinente desde una perspectiva tecnológica.
- **Coherencia con las Precisiones de la SBS a Través del Oficio N° 01690-2024-SBS:** La Comisión fortalece su posición al referenciar el Oficio N° 01690-2024-SBS-PRI, emitido por la misma SBS el 11 de enero de 2024, ya que la SBS indica que "los canales digitales para la provisión de servicios financieros comprenden aquellos medios o plataformas que permiten al usuario interactuar con los productos o servicios de las ESF a través de vías electrónicas o remotas.
- **Extensión Racional de la Ciberseguridad a Operaciones de Uso Masivo (POS y Comercio Electrónico):** Una implicación lógica de esta interpretación es que las transacciones realizadas mediante terminales POS y plataformas de comercio electrónico caen bajo el paraguas del RGSIC, incluso si no requieren un enrolamiento previo y directo del usuario con la entidad bancaria. Por lo tanto, están cubiertas por un marco de ciberseguridad robusto para proteger eficazmente a los consumidores. La Comisión demuestra comprender que la diligencia en ciberseguridad debe trascender la mera existencia de un "enrolamiento" directo en una aplicación bancaria específica.

C) Resolución 2650-2024/SPC-INDECOPI

En este caso, la Sala determinó nuevamente que las operaciones formaban parte del comportamiento regular de consumo de la denunciante y que el Banco demostró su validez, al haberse realizado con la tarjeta habilitada para compras por internet y mediante el ingreso de datos sensibles. Respecto a la aplicación RGSIC, la Sala precisó que no era aplicable al caso, dado que las operaciones se efectuaron en comercios electrónicos y no a través de los canales digitales a los que se refiere dicho reglamento.

Análisis Comparativo: La Urgente Necesidad de Claridad en la Definición de "Canal Digital" y sus Implicaciones para las ESF

La disparidad de criterios entre las resoluciones de la Sala y la Comisión revela una evidente y apremiante ambigüedad interpretativa en torno a la noción de "canal digital" dentro del RGSIC). Esta divergencia no es meramente una cuestión teórica; sus repercusiones son hondas, tanto en la práctica operativa como en la estabilidad jurídica del sector financiero.

Desde la perspectiva de las ESF y otras instituciones financieras, la postura adoptada por la Sala se perfila como la más sensata y sólidamente fundamentada desde el punto de vista legal. La fuerza de esta interpretación radica en su respeto por la autonomía de los marcos normativos y su capacidad para prevenir la aplicación injustificada y extensiva de obligaciones.

1. **Salvaguarda de la Diferenciación Normativa:** La Sala, al interpretar el RGSIC, subraya que la exigencia de un "proceso de enrolamiento previo" (artículo 18°) establece de forma explícita el tipo de canal digital al que está dirigido. Esta lectura mantiene una distinción clara entre las diversas regulaciones existentes. Facilita que las transacciones presenciales (como las realizadas en puntos de venta o cajeros automáticos) o aquellas que se procesan a través de plataformas de terceros (como el comercio electrónico) continúen siendo regidas por las normativas específicas de tarjetas y de protección al consumidor. Estas ya ofrecen medidas de seguridad y mecanismos de responsabilidad adecuados para sus respectivos entornos. La imposición del RGSIC a operaciones que no surgen de un enrolamiento directo con el canal bancario desdibujaría estas fronteras regulatorias, creando confusión.
2. **Prevención de Imposiciones Arbitrarias y Desproporcionadas:** La interpretación de la Sala evita la aplicación forzada de requisitos de autenticación reforzada (característicos de la ciberseguridad) en contextos para los cuales no fueron concebidos ni estructuralmente diseñados. Los sistemas de POS y comercio electrónico operan bajo sus propios protocolos de seguridad y validación, como el CVV (Card Verification Value) y 3D Secure. El CVV es un código de seguridad de tres o cuatro dígitos impreso en la tarjeta, que se solicita en transacciones en línea o por teléfono para verificar que el comprador tiene la tarjeta física en su poder, añadiendo una capa de seguridad contra el fraude. Por su parte, 3D Secure es un protocolo de seguridad que añade un paso de autenticación para las compras en línea, requiriendo que el usuario introduzca una contraseña o un código de un solo uso (OTP) enviado a su teléfono móvil para validar la identidad del usuario de la tarjeta, protegiendo tanto al consumidor como al comercio de transacciones fraudulentas.

Si bien estos son digitales, no implican el mismo nivel de "enrolamiento" o gestión directa de credenciales por parte del banco en el punto de interacción. Exigir la autenticación reforzada del RGSIC en estos escenarios podría acarrear cargas operacionales excesivas, ya que la adaptación de la infraestructura de miles de puntos de venta o plataformas de comercio electrónico para cumplir con requisitos de ciberseguridad diseñados para la banca en línea representaría una inversión económica y logística desproporcionada. Además, podría deteriorar la experiencia del usuario al introducir barreras innecesarias en transacciones cotidianas, impactando negativamente la eficiencia y la fluidez del mercado. Finalmente, generaría incertidumbre jurídica y riesgos de incumplimiento, dado que, sin una base normativa explícita que justifique esta ampliación, las ESF operarían bajo la constante amenaza de sanciones por no cumplir con requisitos que no están claramente estipulados para sus operaciones específicas.

Exigir la autenticación reforzada del RGSIC en estos escenarios podría acarrear:

- **Cargas Operacionales Excesivas:** La implementación de estas medidas de ciberseguridad representaría una inversión económica y logística considerablemente desproporcionada en relación con los beneficios esperados o el riesgo real. Esto implicaría no solo un desembolso significativo de capital para adquirir nuevas tecnologías y herramientas, sino también la necesidad de capacitar al personal, reestructurar procesos y posiblemente contratar expertos adicionales. La magnitud de estos esfuerzos superaría la capacidad actual de la organización, lo que llevaría a una sobrecarga de recursos y a una posible interrupción de las operaciones normales.
 - **Deterioro de la Experiencia del Usuario:** Podría introducir barreras innecesarias en transacciones cotidianas, impactando negativamente la eficiencia y la fluidez del mercado.
 - **Incertidumbre Jurídica y Riesgos de Incumplimiento:** Sin una base normativa explícita que justifique esta ampliación, las ESF operarían bajo la constante amenaza de sanciones por no cumplir con requisitos que no están claramente estipulados para sus operaciones específicas.
3. **Focalización en la Responsabilidad y Diligencia ya Establecidas:** La postura de la Sala confirma que la responsabilidad en casos de fraude relacionados con POS o comercio electrónico debe ser evaluada en consonancia con el RT y el Código de Protección al Consumidor. Estas normativas ya delinear los deberes de monitoreo de transacciones inusuales y la debida diligencia de los proveedores. Este enfoque se considera suficiente y apropiado para la protección de los consumidores en dichos ámbitos.

Los Desafíos Generados por la posición de la Comisión para el Sector Financiero:

En contraste, la Resolución N° 0883-2024/CC1, al adoptar un criterio más amplio y demandante, aunque motivado por una intención de mayor protección, presenta desafíos significativos y riesgos sustanciales para las instituciones financieras:

1. **Creación de Incertidumbre Legal y Desequilibrio:** La expansión del concepto de "canal digital" para incluir "cualquier operación que utilice datos en bits, sin importar el medio" y la inclusión explícita de POS y comercio electrónico bajo el paraguas del RGSIC, a pesar de la ausencia de un "enrolamiento previo", introduce una considerable inestabilidad jurídica. Este cambio interpretativo de gran envergadura, sin una modificación expresa del RGSIC por parte de la SBS, coloca a las ESF en una posición de vulnerabilidad.
2. **Imposición de Obligaciones Desproporcionadas:** Si la interpretación de la Comisión prevalece, los bancos se verían obligados a implementar requisitos de ciberseguridad (posiblemente incluyendo autenticación reforzada) en canales que, por su diseño y funcionalidad, no se corresponden con la lógica del enrolamiento. Esto acarrearía:
 - **Inversiones Masivas:** Requeriría la reingeniería de sistemas, la inversión en nuevas tecnologías y la capacitación del personal para

adaptarse a una normativa que no fue concebida inicialmente para estos canales.

- **Dificultades Operativas y Falta de Viabilidad:** En ciertos escenarios, la aplicación de medidas de ciberseguridad específicas a un POS o a una pasarela de pago de comercio electrónico podría ser técnicamente compleja, inviable o incluso contraproducente para la agilidad de las transacciones.
3. **Uso Cuestionable de un Oficio de la SBS:** Aunque la Comisión invoca el Oficio N° 01690-2024-SBS-PRI, es fundamental recordar que, como ha señalado la propia Sala del Indecopi, los oficios carecen de carácter normativo vinculante. Un oficio puede reflejar la visión de la SBS, pero no posee la autoridad para modificar o extender el ámbito de aplicación de un reglamento vigente. Utilizar un oficio para una expansión tan significativa del alcance de una norma de ciberseguridad, con graves implicaciones en costos y responsabilidades, constituye una debilidad en la argumentación que socava el principio de legalidad y la predictibilidad del marco normativo. Si la SBS considera esencial que los POS y el comercio electrónico estén plenamente cubiertos por el RGSIC, el camino apropiado es la modificación formal de dicho reglamento.

La tensión interpretativa entre ambas resoluciones puso en manifiesto la imperiosa necesidad de que la SBS, en su rol de regulador primario, emita una aclaración explícita y definitiva sobre el concepto y el alcance de “canal digital” dentro de su normativa de ciberseguridad. Desde la perspectiva de la estabilidad del sistema financiero y la previsibilidad jurídica, la interpretación defendida por la Sala emerge como la más razonable y consistente con el diseño y el espíritu original de la regulación. Al mantener una distinción clara entre los diferentes marcos normativos, se evita la imposición de cargas y obligaciones desproporcionadas en entornos que ya disponen de mecanismos de seguridad específicos. Esto, a su vez, contribuye a la eficiencia del mercado y a la seguridad jurídica de todos los actores involucrados. La postura de la Comisión, aunque guiada por la intención de una mayor protección al consumidor, podría desencadenar una espiral de costos e incertidumbres sin contar con un fundamento normativo explícito que la respalde adecuadamente.

4.5. Resultados de la actividad

4.5.1. Discusiones

A) Evaluación de los criterios del Indecopi en la aplicación de normas sobre seguridad de la información y ciberseguridad en consumos no reconocidos

El Indecopi, como organismo encargado de la defensa del consumidor, evalúa la responsabilidad de las ESF en casos de consumos no reconocidos, considerando la aplicación de normas explicadas de forma previa. Para ello, toma en cuenta diversas disposiciones normativas, incluidas aquellas establecidas por la SBS, así como principios generales del Código.

No obstante, en la revisión de las resoluciones analizadas, se evidencia que no existe un criterio uniforme en la aplicación de las disposiciones emitidas por la SBS. Mientras que algunas decisiones del Indecopi han adoptado una interpretación más

restrictiva del RGSIC, señalando que solo se aplica a canales con enrolamiento previo, otras han ampliado su alcance a cualquier canal que utilice datos en bits, lo que genera inseguridad jurídica.

La existencia de interpretaciones disímiles entre la Sala y la Comisión, respecto a la aplicabilidad del RGSIC a las operaciones en ATM, POS y comercio electrónico, no es un mero desacuerdo, sino una manifestación inherente a la autonomía funcional y técnica que caracteriza a los órganos resolutivos del Indecopi.

Esta autonomía les confiere la potestad de interpretar y aplicar la normativa vigente a los casos concretos que conocen, sin injerencias externas, buscando la solución más adecuada conforme a su propio criterio jurídico (Velasquez, 2020). Sin embargo, esta prerrogativa, si bien esencial para la independencia de sus opiniones, se vuelve un punto de análisis crítico cuando genera discrepancias interpretativas internas que afectan la predictibilidad y la seguridad jurídica.

1. La Autonomía de la Comisión y su Interpretación Amplia:

La Comisión ejerció su autonomía funcional y técnica para adoptar una interpretación finalista y expansiva del concepto de "canal digital". Su razonamiento, que profundiza el propósito general de la ciberseguridad y la naturaleza intrínsecamente digital de cualquier operación que maneje "datos en bits" (sin importar el enrolamiento directo).

La Comisión interpretó que el espíritu de la norma, respaldado por pronunciamientos de la SBS, exigía una cobertura más amplia para proteger al consumidor en un entorno de pago digital en constante evolución. En el caso particular, al determinar la responsabilidad del banco, la Comisión pudo argumentar que la operación, al ser "digital" en su esencia, debía someterse a las exigencias de ciberseguridad, responsabilizando a la entidad por no haber aplicado medidas reforzadas, aún cuando la operación no se realizó en un canal con enrolamiento previo. El problema de ello radica en el nivel de expansión que dicha interpretación puede tener al integrar a cualquier plataforma que pueda albergar bits en esta definición y que sobre ello se deban realizar adecuaciones a nivel técnico por parte de las ESF considerando el margen de actuación que tienen las mismas.

2. La Autonomía Jerárquica de la Sala y su Interpretación Restrictiva

Por otro lado, la Sala también ejerció su autonomía funcional y técnica, pero lo hizo desde una posición jerárquica superior y con un enfoque más apegado a la literalidad y especialidad de la norma. La Sala, como última instancia administrativa en la mayoría de estos casos, tiene la potestad de unificar criterios y establecer precedentes.

La Sala, haciendo uso de su función interpretativa decidió que la definición de "canal digital" exige explícitamente un "proceso de enrolamiento previo". En la casuística de consumos no reconocidos en plataformas de comercio electrónico, la Sala determinó que, al no haber un enrolamiento previo del consumidor en el "canal digital" del banco para esa operación específica, el RGSIC no era aplicable. Su autonomía le permitió priorizar la predictibilidad y la legalidad estricta, relegando a los boletines u oficios de la SBS a un carácter no regulatorio y optando por la

aplicación de normativas más específicas como el RT. Su fallo, al revocar la sanción, subraya cómo su interpretación de la autonomía se traduce en una delimitación de la responsabilidad bancaria bajo marcos normativos ya existentes y precisos para cada tipo de transacción.

Esta disparidad de enfoques genera cuestionamientos sobre cuáles son los criterios que utiliza el Indecopi para determinar si una entidad financiera ha cumplido con las medidas de seguridad requeridas y, en consecuencia, si debe asumir la responsabilidad por consumos no reconocidos.

La coexistencia de estas dos interpretaciones, ambas nacidas de la autonomía funcional de los órganos del Indecopi, genera una problemática de seguridad jurídica y predictibilidad para las ESF.

El mismo tipo de operación (un consumo no reconocido en un POS o comercio electrónico) podría ser evaluado bajo criterios diametralmente opuestos dependiendo de qué instancia del Indecopi conozca el caso o qué criterio prevalezca en la revisión. Mientras que la Comisión podría imponer sanciones basándose en la falta de ciberseguridad ampliada, la Sala podría revocar alegando la inaplicabilidad de dicha norma. Esto obliga a los bancos a prepararse para escenarios contradictorios, aumentando sus costos de cumplimiento y su riesgo regulatorio.

La autonomía, si bien permite independencia, debe convivir con la necesidad de uniformidad en la aplicación del derecho. Cuando los órganos inferiores (Comisiones) pueden apartarse de la interpretación de los superiores (Salas) hasta que el caso sea elevado, se crea un ambiente de incertidumbre sobre cuál será el estándar de responsabilidad aplicado finalmente.

En conclusión, la autonomía funcional y técnica del Indecopi es una característica valiosa, pero su ejercicio divergente en la interpretación de "canal digital" en la casuística de consumos no reconocidos pone en relieve la **necesidad imperativa de un criterio unificado y vinculante**. Sin este, el sector financiero se enfrenta a un escenario de inseguridad jurídica que complejiza la gestión de riesgos y la defensa de los derechos de los consumidores.

B) Impacto en las Empresas del Sistema Financiero

El cumplimiento de las medidas de seguridad en consumos no reconocidos ha sido interpretado de manera diferente por el Indecopi, dependiendo de la resolución analizada. La diferencia clave radica en la manera en que la SBS regula los canales digitales y cómo el Indecopi interpreta estos criterios al resolver controversias entre consumidores y entidades financieras.

Por un lado, de acuerdo a lo establecido por el RGSIC se infiere que el acceso a los canales digitales debería tener un proceso de enrolamiento previo y adicionalmente a ello que el entorno sea de forma digital (no indique presencialidad). Sin embargo, en la resolución señalada párrafos arriba la Comisión interpretó el reglamento, incluyendo dentro de la categoría de canales digitales a POS, cajeros automáticos y otros medios, incluso sin enrolamiento previo, el cual fue tomado a raíz de

pronunciamientos por parte de la SBS; sin perjuicio de no haberse modificado el RT o el RGSIC.

Esta falta de alineación entre el Indecopi y la SBS genera problemas en la aplicación de las normas, ya que las ESF podrían cumplir con los requisitos establecidos en el RT, pero serían sancionadas por el Indecopi bajo una interpretación distinta o amplia, tomando en cuenta los alcances del RGSIC.

Otro aspecto clave es si el Indecopi está obligado a considerar todos los pronunciamientos de la SBS, incluyendo aquellos que no tienen carácter normativo, como boletines informativos o comunicados.

Si bien la SBS es el organismo especializado en la regulación del sistema financiero, no todas sus comunicaciones tienen la misma jerarquía. La Sala no tomó en cuenta que los boletines informativos de la SBS, ya que indicaba que no pueden ser utilizados como criterio normativo, ya que no tienen carácter vinculante. Sin embargo, la Comisión adoptó una interpretación distinta, considerando ciertos pronunciamientos de la SBS para ampliar la aplicación del RGSIC.

Esto demuestra que el Indecopi no está obligado a seguir todos los pronunciamientos de la SBS y que, en la práctica, selecciona aquellos criterios que considera relevantes según el caso concreto.

Las resoluciones del Indecopi reflejan criterios dispares en la aplicación del RGSIC, lo que ha generado incertidumbre sobre su correcta implementación en el sistema financiero. Estas diferencias de interpretación tienen consecuencias significativas en la operatividad del sistema financiero. La postura tomada por la Sala permitiría que los bancos y otras entidades financieras ajusten sus procesos de seguridad de acuerdo con el canal utilizado, evitando la imposición de medidas innecesarias en operaciones que ya cuentan con mecanismos de validación específicos.

Por el contrario, la interpretación realizada por la Comisión requeriría que las ESF implementen controles de ciberseguridad más exigentes en todas las transacciones electrónicas, lo que podría derivar en mayores costos operativos, demoras en la autorización de pagos y posibles conflictos con otras regulaciones vigentes, como las establecidas en el RT.

Además, la falta de uniformidad en la interpretación del RGSIC también puede generar inseguridad jurídica y conflictos regulatorios. Mientras que la primera resolución mantiene coherencia con el marco regulatorio existente, al integrar su aplicación con el RT, la segunda resolución introduce un cambio interpretativo sin que haya una modificación explícita en la norma, lo que dificulta su implementación efectiva y podría llevar a sanciones contradictorias por parte de las instituciones.

Adicionalmente consideramos que es fundamental que el Indecopi mejore su enfoque en la aplicación de la normativa financiera, reconociendo que las problemáticas del consumidor financiero requieren un tratamiento diferenciado del que se aplica en otros sectores. Esto se debe a que las operaciones y productos financieros poseen características más complejas, lo que exige un mayor grado de especialización en la interpretación de la regulación.

En este sentido, la doctrina especializada ha señalado la importancia de un enfoque diferenciado para la protección del consumidor financiero. Vodanovic (2016) resalta que los productos y servicios financieros son distintos a otros bienes y servicios del mercado. En el Perú, la protección del consumidor financiero se encuentra incluida dentro de las normas generales de protección al consumidor, lo que implica que el Indecopi debe supervisar estos casos, a pesar de que la regulación financiera tiene particularidades que requieren un conocimiento más especializado. Dado que los productos financieros son sofisticados, se necesita una comprensión más profunda y una aplicación técnica de las normas que los regulan.

Este análisis refuerza la idea de que el Indecopi debe abordar los casos de ciberseguridad en el sector financiero con mayor precisión y conocimiento técnico, garantizando que las resoluciones sean consistentes con el marco normativo especializado en banca y finanzas.

Dada la falta de uniformidad en la interpretación del RGSIC, la opinión de la Sala parece ser la más adecuada para garantizar una aplicación coherente y eficiente de la normativa. Este enfoque evita cargas operativas excesivas para las ESF, al mismo tiempo que asegura que las medidas de seguridad sean proporcionales y acordes con la naturaleza de cada canal de transacción.

Además, la necesidad de un enfoque especializado en la regulación del consumidor financiero, como lo señala Vodanovic, es un punto clave que debe ser tomado en cuenta en futuras interpretaciones. La complejidad de los productos financieros y los riesgos asociados a su uso exigen que la regulación se aplique con criterios técnicos y específicos, evitando interpretaciones amplias que puedan generar conflictos normativos y costos innecesarios.

Por ello, ante el escenario regulatorio actual, resulta imprescindible que el Indecopi tome una postura uniforme para sus pronunciamientos y que la SBS establezca criterios claros que permitan evitar contradicciones en la aplicación del RT así como la de ciberseguridad, asegurando que la normativa financiera brinde claridad tanto a los consumidores como a las ESF. Un marco normativo bien definido y aplicado con rigurosidad técnica contribuirá a fortalecer la confianza en los canales digitales y garantizar una protección efectiva a los usuarios del sistema financiero.

C) Impacto de la Discrepancia Interpretativa en los Consumidores de Servicios Financieros Digitales

La divergencia de criterios entre la Sala y la Comisión del Indecopi, así como la postura de la SBS, sobre la definición de "canal digital" y la aplicación del RGSIC a operaciones en ATM, POS y comercio electrónico, genera un impacto significativo y predominantemente negativo en los consumidores de servicios financieros. Este impacto se manifiesta principalmente en la incertidumbre sobre el nivel de protección aplicable, la complejidad en la resolución de controversias y la potencial afectación a la confianza en el ecosistema digital.

1. Mayor Complejidad y Riesgo en la Resolución de Controversias por Consumos No Reconocidos:

Riesgo de Resultados Contradictorios: La principal consecuencia para el consumidor es que el resultado de su reclamo por un consumo no reconocido (ej., un fraude en POS o e-commerce) puede depender de la instancia del Indecopi que resuelva su caso (Comisión vs. Sala) o del criterio que prevalezca en un momento dado. Un consumidor no debería ver sus derechos afectados por una discrepancia interpretativa entre las autoridades.

- **Prolongación de los Procesos:** Esta discrepancia fomenta la litigiosidad. Si una Comisión resuelve a favor del consumidor bajo una interpretación amplia (aplicando ciberseguridad), el banco probablemente apelará ante la Sala, buscando la interpretación restrictiva. Si la Comisión resuelve a favor del banco, el consumidor apelará. Esto alarga innecesariamente los procesos de resolución, generando mayor desgaste, tiempo y costos (indirectos) para el consumidor que busca la reparación de un perjuicio.
- **Asimetría de Información y Conocimiento Jurídico:** El consumidor ya se encuentra en una posición de asimetría de información frente a la entidad financiera. Si además debe navegar por complejas interpretaciones normativas y divergencias entre órganos administrativos, su capacidad para defender sus derechos se ve seriamente comprometida.

2. Potencial Deterioro de la Confianza en los Servicios Financieros Digitales:

- **Percepción de Impunidad o Desprotección:** Si los consumidores perciben que las reglas de juego son inconsistentes o que, en ciertas operaciones "digitales", la protección en materia de ciberseguridad es menor a la esperada, esto puede erosionar su confianza en la seguridad de las operaciones que realicen.
- **Freno a la Inclusión Financiera Digital:** La desconfianza puede disuadir a los consumidores de adoptar o utilizar plenamente los canales digitales (como pagos con billeteras digitales en comercios, o compras en línea), lo cual contraría los objetivos de modernización e inclusión financiera. Un sistema donde la ciberseguridad es ambigua es un sistema que genera recelo.
- **Fomento de la Desconexión con la Regulación:** Si la aplicación de la normativa parece caprichosa o contradictoria, el consumidor podría perder la fe en la capacidad de las autoridades (Indecopi y SBS) para protegerlo eficazmente en el ámbito digital.

D) Impacto en el principio de predictibilidad: Análisis de las Posiciones Contradictorias sobre la Aplicación del RGSIC.

La divergencia interpretativa en torno a la forma de aplicación del RGSIC particularmente en el contexto de operaciones no reconocidas genera una preocupación significativa por la vulneración del principio de predictibilidad. Este principio fundamental del derecho administrativo exige que los consumidores y las ESF confíen en la estabilidad y coherencia de los criterios aplicados por la administración pública en su actuación.

En el ordenamiento jurídico peruano, dicho principio se encuentra dispuesto en el Título Preliminar del TUO de la Ley N° 27444, LPAG, **se deduce de sus principios cardinales, como el de predictibilidad y seguridad jurídica.**

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

Como señala Morón (2021), la administración pública debe actuar de manera tal que genere en los administrados una expectativa razonable y fundada sobre la continuidad de sus decisiones y criterios interpretativos, permitiendo la planificación y el ejercicio de derechos y obligaciones con certeza.

Pero además la misma área de estudios económicos del Indecopi (2000) ha señalado lo siguiente:

la Administración Pública arroje resultados predecibles, es decir consistentes entre sí. La administración no debe hacer diferencias en razón de las personas –imparcialidad y neutralidad-, y los ciudadanos deberían, al iniciar un trámite, tener una expectativa certera de cuál será el resultado final que dicho procedimiento arrojará (p. 23).

Cuando los órganos administrativos exhiben interpretaciones contradictorias sobre una misma normativa, se socava directamente la previsibilidad de sus decisiones y, por ende, la predictibilidad. Las ESF, al actuar de buena fe y ajustar su conducta a lo que razonablemente esperan de la administración, construyen una confianza en la continuidad y uniformidad de los criterios interpretativos. Sin embargo, la aparición de fallos divergentes, como los observados entre la Sala y la Comisión del Indecopi respecto al RGSIC, rompe esta expectativa legítima.

Esta situación crea un escenario de inseguridad jurídica. Las ESF se ven expuestas a un riesgo regulatorio incrementado, ya que el mismo tipo de operación puede ser evaluado bajo distintos parámetros, llevando a resultados contradictorios y potencialmente a sanciones inesperadas. A falta de un criterio uniforme por parte de los órganos resolutivos del Indecopi, en particular sobre la definición y el alcance de "canal digital" para aplicar las obligaciones del, impide a las ESF a adaptar con certeza sus procesos y controles de seguridad. Esto es especialmente crítico en operaciones como las de comercio electrónico, donde la responsabilidad por consumos no reconocidos se vuelve un punto de disputa constante.

El principio de predictibilidad busca proteger al administrado frente a cambios bruscos o sorpresivos en la actuación administrativa que no estén debidamente justificados o que contravengan una expectativa fundada. Cuando la autoridad (Indecopi) no mantiene una línea interpretativa clara y uniforme, se genera un ambiente de incertidumbre que afecta directamente la planificación estratégica de las ESF, sus inversiones en tecnología y seguridad, y, en última instancia, la fluidez y el desarrollo del sector financiero digital.

5. Conclusiones

El Indecopi no mantiene un criterio uniforme en la aplicación del RGSIC a los consumos no reconocidos, lo que genera incertidumbre jurídica en la interpretación de las normas aplicables. Dependiendo de la resolución, se han adoptado enfoques más restrictivos o más amplios sobre qué operaciones deben ser consideradas dentro de la regulación de seguridad de la información.

Existe una discrepancia entre la interpretación del Indecopi y la regulación establecida por la SBS, en especial en relación con la definición de canal digital y la obligatoriedad de la autenticación reforzada en ciertos entornos. Esta falta de alineación genera riesgos de sanciones para las ESF, incluso cuando cumplen con las disposiciones establecidas por la SBS.

La ausencia de un criterio unificado y claro en la definición de "canal digital" y la aplicación de las normas de ciberseguridad tiene un impacto directo y perjudicial en los consumidores. Crea un ambiente de incertidumbre sobre sus derechos y el alcance de la protección, complejiza y alarga la resolución de sus reclamos por fraudes, y potencialmente socava su confianza en la seguridad y la fiabilidad de un ecosistema financiero cada vez más digitalizado. Para una protección efectiva del consumidor, es indispensable que las autoridades competentes, siguiendo la línea de la Sala (dada su mayor coherencia normativa), logren una definición precisa y vinculante que brinde predictibilidad y seguridad a todas las partes involucradas.

6. Recomendaciones

Es necesario que, ante futuras situaciones el Indecopi mantenga una interpretación lineal y sostenida conforme a las disposiciones establecidas por la SBS y a su vez que la regulación de la SBS sea más clara y determine los casos en los que apliquen las normas de seguridad de la información y ciberseguridad, para evitar contradicciones que puedan generar sanciones desproporcionadas a las ESF.

Conforme a lo señalado en el D.L. N° 1033, dentro de las facultades del Indecopi la Sala es el órgano de última instancia en la vía administrativa y posee la facultad legal para establecer **precedentes de observancia obligatoria** sobre los criterios interpretativos de la normativa de protección al consumidor y las regulaciones sectoriales que le competen.

Esta potestad se rige principalmente por:

1. **Ley N° 27444 (TUO de la LPAG):** El Principio de Predictibilidad y los artículos que regulan la **declaración de precedentes administrativos** confieren a los órganos resolutivos la capacidad de establecer criterios

interpretativos que sean vinculantes para sí mismos y para los órganos inferiores (las Comisiones).

2. **Normativa Propia del INDECOPI:** Para que un criterio se convierta en precedente de observancia obligatoria (precedente vinculante *formal*), la Sala debe:
 - **Declararlo expresamente** en la parte resolutive de la resolución.
 - **Detallar el criterio** y la fundamentación jurídica que lo sustenta.
 - **Publicarlo en el Diario Oficial El Peruano.**

Si la Sala decidiera, en un caso como el de la definición de "canal digital" para el RGSIC, que su interpretación restrictiva es la correcta, podría elevar la resolución a la categoría de precedente. De hacerlo, su criterio sería obligatorio para la Comisión y para todos los órganos del INDECOPI, poniendo fin a la discrepancia interpretativa interna y garantizando la predictibilidad en el sistema.

Dado que las resoluciones del Indecopi han evidenciado vacíos normativos en la definición de canal digital, es labor de la SBS aclarar formalmente el alcance de este concepto, estableciendo criterios específicos para evitar interpretaciones expansivas o restrictivas según el caso. Al respecto, el 26 de junio del 2024 la SBS dispuso una serie de disposiciones normativas en el RT a través de la Resolución 2286-2024 especificando la obligación del cumplimiento del RGSIC para todas las operaciones con tarjeta, estableciendo un margen de adecuación hasta julio del 2025. A raíz de la publicación, el Indecopi ha tomado en cuenta estas nuevas disposiciones dentro de sus pronunciamientos; sin embargo, tomando en cuenta la fecha de publicación, así como la entrada en vigencia de las disposiciones aplicables al RGSIC (año 2022) y las nuevas disposiciones (año 2025), este actuar fue tardío y ha permitido que la interpretación por parte de las instituciones financieras y del Indecopi sea disconforme

Dado que la interpretación del Indecopi no es uniforme, las ESF (incluida el Banco) tuvieron que adoptar estrategias de defensa basadas en la interpretación más restrictiva del RGSIC, demostrando que cumplen con los criterios establecidos por la SBS y que una ampliación de su alcance podría vulnerar principios de seguridad jurídica.

En vista de lo señalado, la falta de un criterio uniforme en la aplicación de las normas de ciberseguridad en consumos no reconocidos representa un riesgo regulatorio para las ESF.

Por ello, es fundamental que la SBS tome acciones decisivas para eliminar la ambigüedad dentro de la interpretación de la normativa, lo que ha permitido la existencia de criterios contradictorios entre la Sala y la Comisión del INDECOPI. El primer paso es que la Sala del INDECOPI, ante casos similares, ejerza formalmente su potestad, establecida en el D.L. N° 1033 y la Ley N° 27444, para declarar un precedente de observancia obligatoria que fije la interpretación restrictiva del RGSIC. Este paso inmediato unificaría el criterio dentro de la propia institución y restablecería la predictibilidad del marco sancionador.

Sin embargo, la solución de fondo requiere una intervención directa y oportuna de la SBS. A pesar de la reciente modificación al RT (Resolución SBS N° 2286-2024), que remite el proceso de autenticación al Artículo 19 del RGSIC (Resolución SBS N°

504-2021) y a los estándares EMVCo², persiste un vacío normativo estructural que debe ser corregido mediante una modificación directa a la Resolución SBS N° 504-2021. Este vacío se manifiesta en varios puntos:

- **Definición de Canal Digital:** El RGSIC aún mantiene una definición amplia de "canal digital" que no determina taxativamente en qué casos se requiere la aplicación del enrolamiento y la autenticación reforzada.
- **Alcance de la Obligación:** La normativa no especifica qué tipos de operaciones con tarjetas están sujetas a la aplicación del Artículo 19 del RGSIC, más allá de los lineamientos generales.
- **Restricción Tecnológica:** La regulación se limita a mencionar el código dinámico y el CVV DINÁMICO para POS y comercios electrónicos, restringiendo la posibilidad de que las ESF adopten otros estándares técnicos y medidas de seguridad avanzada que podrían ser más seguros o eficientes bajo los estándares EMVCo.

Por lo tanto, es necesario que la SBS modifique el RGSIC para establecer lineamientos que definan cuándo aplica el enrolamiento y adopten un marco de seguridad tecnológicamente neutral. Este enfoque permitirá a las ESF cumplir con los criterios de seguridad sin caer en interpretaciones disconformes, lo que garantizará la estabilidad del sistema financiero y una protección efectiva y previsible para los consumidores.

² EMVCo es un estándar global de seguridad para pagos con tarjeta que lleva el nombre de las tres compañías que crearon la primera versión: Europay, Mastercard y Visa. EMVCo es una organización creada por varias compañías líderes en la industria de pagos, incluyendo American Express, Discover, JCB, Mastercard, UnionPay y Visa." (Scribd, s.f., párr. 1-2).

7. Bibliografía

ÁREA DE ESTUDIOS ECONÓMICOS DEL Indecopi (2000). Impulsando la Simplificación Administrativa: Un reto pendiente. Documento de Trabajo N.º 002-2000, publicado el 10 de abril del 2000 en el Diario Oficial El Peruano, p. 23.

Modificaciones RT de Crédito y Débito, aprobadas por la Resolución SBS N° 2286-2024

Morón, J. (2021). Comentarios a la Ley del Procedimiento Administrativo General. Texto Único Ordenado de la Ley N° 27444 (Decreto Supremo N° 004-2019-JUS). Edición conmemorativa por los 20 años de vigencia de la LPAG.

RT de Crédito y Débito, aprobado mediante la Resolución SBS N° 6523-2013.

Instituto Nacional de Defensa de la Competencia y la Propiedad Intelectual (2024). Resolución N° 0201-2024/SPC. <https://servicio.indecopi.gob.pe/buscadorResoluciones/getDoc?docID=workspace://SpacesStore/9cf8747d-c048-42eb-a4ae-221bec788e61>

Instituto Nacional de Defensa de la Competencia y la Propiedad Intelectual (2024). Resolución N° 0883-2024/CC1. <https://servicio.indecopi.gob.pe/buscadorResoluciones/getDoc?docID=workspace://SpacesStore/45414987-8b09-459b-bf0e-0e8d2b8adfd3>

Instituto Nacional de Defensa de la Competencia y la Propiedad Intelectual (2024). Resolución N° 2650-2024/SPC-INDECOPI. <https://servicio.indecopi.gob.pe/buscadorResoluciones/getDoc?docID=workspace://SpacesStore/cdf1cce1-1cd3-431f-9df9-2f9b8cce7890>

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 (2022). Autenticación reforzada: mayor seguridad para operaciones que puedan generar perjuicio al usuario. Boletín SBS, julio 2022. <https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1222?title=Autenticaci%C3%B3n%20reforzada:%20mayor%20seguridad%20para%20operaciones%20que%20puedan%20generar%20perjuicio%20al%20usuario/1000>.

SBS (2022). Entidades que provean operaciones en canales digitales deben reforzar la autenticación del usuario. Nota de Prensa <https://www.sbs.gob.pe/noticia/detallenoticia/idnoticia/2615>

SBS (2022). Oficio N° 36482-2022-SBS. Fecha: el 31 de agosto de 2022.

SBS (2024). Oficio N° 01690-2024-SBS. Fecha: el 11 de enero de 2024.

Zapata de la Piedra, K. G., Calle Cabrera, P. S., Chirinos Quiroz, R. A., Guzmán Palomino, J. A., Melitón Magallanes, L. C., Rosadio Camahualí, J. E., Rosales

Vicente, K. M., & Soto Vilcapoma, N. L. (2015). Entrevista a Ljubica Vodanovic Ronquillo: Balances y perspectivas en torno a la protección del consumidor financiero. *Revista de Actualidad Mercantil*, (4), 288-292. Recuperado a partir de <https://revistas.pucp.edu.pe/index.php/actualidadmercantil/article/view/14966>.

Velásquez, R. (2020). El Indecopi como organismo constitucional autónomo: razones sobre el proyecto de modificación constitucional. *THEMIS Revista De Derecho*, (78), 91-115. <https://doi.org/10.18800/themis.202002.005>

EMV Conceptos y Términos Fundamentales. (s.f.). Scribd. Recuperado de <https://es.scribd.com/document/804072261/EMV-Conceptos-y-terminos-fundamentales>