Autores:
Alonso Morales Acosta
Karina Seminario Coronado

CIBERSEGURIDAD FINANCIERA Y CONSUMIDOR EN LA ERA DIGITAL

CIBERSEGURIDAD FINANCIERA Y CONSUMIDOR EN LA ERA DIGITAL

Financial cybersecurity and consumer protection in digital era

Autores: Alonso Morales Acosta[1]

Karina Seminario Coronado[2]

SUMARIO:

Resumen

El uso masivo de canales digitales en el sistema financiero ha traído consigo múltiples beneficios, tales como la inmediatez y la ampliación de los servicios financieros tradicionalmente ofrecidos. Sin embargo, también ha generado riesgos significativos: los delitos cibernéticos han aumentado en complejidad y frecuencia, afectando tanto a consumidores como a proveedores. En este contexto, la ciberseguridad constituye una responsabilidad compartida por parte de ambos actores en la relación de consumo. En el presente artículo, haremos un breve recuento de las medidas del proveedor financiero y consumidor para neutralizar ataques de ciberdelincuentes, y el análisis que autoridades como el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (en adelante, el INDECOPI) y la Superintendencia de Banca y Seguros (en adelante, la SBS) efectúan, en aras de determinar el traslado de responsabilidad en la comisión de un ciber delito.

[1] Abogado por la Facultad de Derecho de la PUCP. Magíster en Derecho Civil y Comercial por la Universidad Nacional Mayor de San Marcos. Estudios de Doctorado en Derecho por la Universidad de Salamanca. Profesor Titular en la Facultad de Derecho de la Universidad de Lima. Socio Principal y Jefe del área de Protección al Consumidor y Derecho de la Competencia de Torres y Torres Lara Abogados. Correo de contacto: alonso.morales@tytl.com.pe

[2] Abogada por la Universidad de Lima. Máster Universitario en Derecho, Empresa y Justicia por la Universidad de Valencia. Máster Universitario en Derecho Digital por la Universidad Internacional La Rioja de España (en curso). Los comentarios expuestos por la autora en el presente artículo son efectuados a título estrictamente personal y por supuesto que son debatibles. Correo de contacto: karina.seminario.c@gmail.com

Palabras clave

Ciberseguridad/ consumo digital/ Protección al Consumidor/ autenticación reforzada/ ingeniería social/ ciberdelitos/ fraude financiero/ validación biométrica/ patrón de consumo.

Abstract

The widespread use of digital channels in the financial system has brought multiple benefits, such as immediacy and the expansion of traditionally offered financial services. However, it has also generated significant risks: cybercrimes have increased in both complexity and frequency, affecting consumers and providers alike. In this context, cybersecurity constitutes a shared responsibility between both actors in the consumer relationship. This article provides a brief overview of the measures taken by financial providers and consumers to neutralize cybercriminal attacks, as well as the analysis conducted by authorities such as INDECOPI and the SBS, aimed at determining the allocation of responsibility in the commission of a cybercrime.

Keywords

Cybersecurity, digital consumption, Consumer Protection, strong authentication, social engineering, cybercrimes, financial fraud, biometric validation, consumption patterns.

I. INTRODUCCIÓN

Con la llegada de la pandemia, el mundo tal y como lo conocíamos cambió radicalmente. Si bien veníamos encaminados a la digitalización, en particular de los servicios financieros, la pandemia incrementó cuantitativa y cualitativamente la digitalización de las relaciones jurídicas y económicas. En ese sentido, desde la incorporación del trabajo remoto, y la digitalización de muchas de nuestras actividades diarias, lo que antes eran transacciones presenciales que formaban parte de nuestra rutina, hoy se han convertido en múltiples interacciones virtuales gestionadas en cuestión de minutos. El consumo digital se ha vuelto parte intrínseca de nuestra vida, siendo la gestión de nuestras finanzas personales y la adquisición de bienes y servicios en línea, parte de nuestro día a día. Por ello hoy, la ciberseguridad, lejos de ser un asunto exclusivo de expertos en tecnología, se ha convertido en un tema fundamental que nos atañe a todos. En ese contexto, los pagos digitales en Perú han crecido 884 % desde 2019, impulsando la inclusión financiera y reduciendo el uso del efectivo. Hoy, el 72 % de adultos usan billeteras digitales, confirmando el crecimiento sostenido de la digitalización financiera. El Estudio de Medios de Pago en el Perú de 2025 de NTT Data[3], revela que para el 2027 menos del 28% de los pagos se harán en efectivo, y que incluso en los puntos de venta físicos, las ventas serán por canales digitales. La región Chile, por ejemplo, es el país con menor uso de efectivo, con un 12% de la población que lo ocupa como principal alternativa de pago en el 2022[4].

[3] Verderas, Pablo, Luis Olmedo, Nacho Núñez et al. "Estudio Medios de Pago en el Perú 2025". NTT DATA, 2025. (consultora multinacional con presencia en más de 50 países) https://pe.nttdata.com/documents/NTT%20DATA%20-%20PAYMENT.pdf.

[4] Cifuentes, Martín. "¿El fin del dinero en efectivo? Sólo un 12% de los chilenos lo usa para pagar". La Tercera, 23 de agosto de 2023. https://www.latercera.com/piensa-digital/noticia/el-fin-del-dinero-en-efectivo-solo-un-12-de-los-chilenos-lo-usa-para-pagar/IAPJQA6BS5EZXFQ6PNYAZQOPA4.

Por ello, resulta trascendental el esfuerzo de las empresas del sistema financiero, ya que, en su afán de lograr la inclusión financiera, se han servido de la tecnología para masificarla. De ahí que hoy se haya generalizado la idea de lograr una inclusión financiera digital, a través del uso adecuado de las nuevas tecnologías. Este escenario genera una responsabilidad compartida entre quienes ofrecen los servicios digitales y quienes los utilizan.

En efecto, en esta responsabilidad compartida hay roles de diligencia que corresponden a las categorías de proveedor y consumidor. El mercado exige que el proveedor afronte los riesgos que plantea el uso de la tecnología mediante un cambio de paradigma, pasando de la tradicional seguridad reactiva, que abordaba incidentes individuales después de que ocurrían, a la implementación de medidas proactivas y preventivas a nivel global. Es decir, en lo posible, tratar de adelantarse y evitar que se consuman los daños provenientes de actos delictuosos, de obsolescencia tecnológica, de los sistemas (software) o de equipamiento (hardware o de cualquier otro proveniente de la naturaleza o de terceros).

Es claro que muchos de estos pueden tener repercusiones de gran alcance, en tanto, una sola falla podría tener consecuencias masivas, afectando a un vasto número de individuos en simultáneo y pudiendo paralizar países enteros. El propósito de este análisis es precisamente ese: advertir de la necesidad de implementar el cambio de paradigma en ciberseguridad, precisar cuáles son los riesgos más comunes y explicar sucintamente, las medidas que han implementado las autoridades sectoriales de nuestro país, relacionadas principalmente al sistema financiero.

Desde luego, no podemos ignorar que al consumidor también le corresponde una conducta de diligencia ordinaria, si quiere transitar con el menor riesgo por los dispositivos y sistemas digitales; en ese sentido, tienen que informarse también -adecuadamente- sobre los usos y referencias en seguridad que el mercado le ofrece, así como mantener una actitud muy prudente.

II. EL PANORAMA DE LA CIBERCEGURIDAD HOY

Históricamente, el fraude, robo o la suplantación de identidad coincidían en la presencia física del autor y la víctima, junto con algún tipo de recurso de engaño, intimidación o amedrentamiento y, en su caso, la fuerza bruta necesaria para controlar a la víctima. Pensemos en el típico carterista que operaba en un mercado concurrido para robar la billetera o el estafador que necesitaba interactuar directamente con su víctima con la finalidad de timarla.

Hoy estas conductas siguen acontenciendo, pero naturalmente han mutado a nuevas modalidades, lo cual se refleja en las denuncias por ciberdelitos que se han multiplicado significativamente desde el 2020, e incluso de año a año. Ello puede notarse en particular por el incremento de denuncias producido entre el 2023 y 2024. En efecto, en el 2024 hubo un aumento de más del 40 % en denuncias totales (42 000 casos) respecto a 2023[5]. Lo delicado de la situación actual es que el daño o perjuicio se genera mediante una acción virtual (no presencial), es decir, sin presencia física de la víctima, lo que permite un mejor ocultamiento, camuflaje o dificultad en la trazabilidad de la operación; a lo cual se suma

[5] Chávarry, Freddy. "Fraudes digitales y suplantación de identidad: expertos analizan cifras de la PNP sobre impacto de la ciberdelincuencia". RPP Noticias, 3 de marzo de 2025. https://rpp.pe/peru/actualidad/fraudes-digitales-y-suplantacion-de-identidad-expertos-analizan-cifras-de-la-pnp-sobre-impacto-de-la-ciberdelincuencia-noticia-1620813.

un impacto masivo (ya no de alcance singular), afectando a millones de personas en segundos y un alcance trasfronterizo, desde cualquier parte del mundo, hacia el lugar donde se produce la afectación. Basta tener una computadora y la información necesaria para encontrar la forma de vaciar -en cuestión de minutos- cuentas bancarias enteras desde otro país.

Esta mutación de las amenazas, de lo singular a lo masivo, de lo visible a lo invisible, desde lo próximo a lo remoto, ha alterado profundamente el escenario de riesgos. Ya no hablamos de incidentes aislados, sino de potenciales catástrofes digitales que exigen medidas de ciberseguridad proactivas y sistémicas. La capacidad de un atacante para comprometer la información de un gran número de individuos simultáneamente, a través de una única brecha de datos, es una realidad que exige una vigilancia constante y una adaptación continua de las estrategias de protección.

III. EL ORIGEN DE LOS DAÑOS PATRIMONIALES

3.1 Los ciberdelitos y sus móviles: dinero, diversión, ideologías

¿Qué impulsa a los ciberdelincuentes a cometer estos actos? Si bien el principal motivo es el dinero, ya sea a través de la apropiación directa de fondos o la extorsión, existen otras razones que también alimentan esta actividad ilícita. Algunos ciber atacantes buscan la diversión o el prestigio dentro de comunidades clandestinas, mientras que otros actúan por motivos ideológicos o incluso por venganzas personales.

Comprender esta diversidad de motivaciones es crucial, pues permite adoptar un enfoque más holístico de la ciberseguridad. Si los objetivos de los atacantes varían, también lo harán los tipos de ataques y sus blancos. Un ataque ideológico, por ejemplo, podría buscar la destrucción de datos o la vergüenza pública, mientras que uno motivado financieramente se centrará en el robo de los datos de acreditación o credenciales bancarias, para luego acceder a los fondos de la víctima. Esto significa que las estrategias de seguridad deben ser multifacéticas, protegiendo no solo los activos financieros, sino también la reserva y la reputación personal, la integridad de los datos y la continuidad operativa de la plataforma digital.

3.2 Vulnerabilidades internas del proveedor: obsolescencia tecnológica, fallas humanas y eventos fortuitos

Naturalmente, no siempre las afectaciones tienen su origen en móviles maliciosos de terceros que desean aprovechar los datos para dañar económicamente, sino que estos pueden provenir de las fallas originadas por la obsolescencia del hardware o software, por errores humanos, o por casos fortuitos o de fuerza mayor, tales como guerras, vandalismos, motines, insubordinaciones, manifestaciones violentas, entre otros.

La obsolescencia tecnológica, por ejemplo, ocurre cuando los sistemas y programas no se actualizan, dejando brechas de seguridad que pueden ser explotadas. Las fallas humanas, como el error de un empleado al hacer clic en un enlace malicioso o al usar una contraseña débil, son también una causa significativa de incidentes de seguridad. Incluso los eventos naturales, como cortes de energía o desastres, pueden interrumpir los sistemas y crear oportunidades para los atacantes.

En efecto, los eventos mencionados pueden generar daños por sí solos, o ser también la oportunidad para que los ciber atacantes aprovechen la vulnerabilidad que se ha presentado. El error humano y la obsolescencia tecnológica son, en muchos casos, vectores de ciber amenazas tan importantes, sino más, que los ataques externos sofisticados. Esta

realidad sugiere que la ciberseguridad no se limite a defenderse de los hackers, sino que también gatille la implementación de procesos internos sólidos, la realización de actualizaciones regulares del sistema y una educación continua del personal del proveedor, así como del usuario. Si la falta de precaución y las fallas humanas son una causa recurrente, la capacitación y la concientización se convierten en una primera línea de defensa. En ese contexto, se resalta la importancia crítica de mantener el software y los sistemas actualizados para neutralizar el riesgo que representa la obsolescencia tecnológica. Esto amplía el enfoque circunscrito sobre las amenazas puramente externas, a una visión más holística que se fija también en las vulnerabilidades internas que pueden mitigarse mediante el comportamiento diligente del proveedor y un mantenimiento tecnológico constante.[6]

IV. RIESGOS EN EL PROCESAMIENTO DE OPERACIONES PRESENCIALES Y NO PRESENCIALES

4.1 En operaciones presenciales

La forma en que interactúan las personas con los servicios digitales influye directamente en el nivel de riesgo. Tradicionalmente, la presencialidad se ha asociado con un menor riesgo, ya que implica una interacción física y, a menudo, la verificación de identidad mediante documentos o datos biométricos. Sin embargo, la idea de que la presencia física elimine por completo el riesgo es un error, pues incluso en situaciones presenciales, como las operaciones en ventanilla, podrían ser efectuadas por un estafador que suplanta al cliente; tampoco están exentos los que se realizan en un cajero automático o mediante un terminal en el punto de venta (POS), que podrían ser aprovechadas para operaciones fraudulentas mediante la "clonación" o un "cambiazo"[7]. La posibilidad de fraudes encuentra inclusive un terreno fértil en las operaciones que se realizan en establecimientos comerciales de poco monto, ya que el Reglamento de Tarjetas de Crédito y Débito al exceptuar a los micropagos de "autenticación reforzada" (identificación con DNI o digital), ha priorizado la celeridad de las transacciones sobre la imposición de medidas de seguridad adicionales que puedan dilatar el procesamiento de la operación. Se entiende que por los pequeños importes autorizados, el sistema está interiorizando estos riesgos dentro de sus costos.

Como puede apreciarse, en el mundo moderno ya no existen operaciones presenciales que se registran o realizan solo en soporte físico, pues no hay una operación en la ventanilla de un banco que se realice sin un dispositivo digital (Ej.: POS); empero cabe recordar que la presencia física nunca ha neutralizado en su totalidad la posibilidad de un fraude, aunque sí podía limitar la extensión del daño.

4.2 En operaciones no presenciales

Corresponde referirnos ahora a aquellas conductas más usuales de los ciberdelincuentes, que aprovechan las vulnerabilidades del entorno digital para engañar a los consumidores

[6] SOTESA. "Consejos de ciberseguridad para proteger tus equipos". Sotesa. https://sotesa.com/consejos-de-ciberseguridad/.

[7] Clonación: es la copia ilegal de la información contenida en una tarjeta bancaria (banda magnética o chip) mediante dispositivos electrónicos, con el fin de fabricar una réplica y usarla para realizar transacciones no autorizadas. Cambiazo: Es una modalidad de fraude en la que el delincuente sustituye la tarjeta original del usuario por otra (falsa o inservible), generalmente durante una distracción en cajeros automáticos o comercios, para quedarse con la tarjeta verdadera y usarla de manera fraudulenta.

y obtener acceso a su información o dinero. A continuación, presentamos algunas de las formas más frecuentes de ingeniería social[8] en el consumo digital:

- **Phishing:** se produce cuando el ciberdelincuente simula actuar en nombre de una entidad de confianza (un banco, una tienda en línea, una institución pública) para engañar a la víctima, con la finalidad de que revele información sensible. Esto puede ocurrir a través de correos electrónicos, mensajes de texto, llamadas telefónicas, páginas web o plataformas simuladas.

    - Ejemplo: Recibir un correo electrónico que parece ser del banco de la víctima, alertándola de un "problema de seguridad" en su cuenta y pidiéndole que haga clic en un enlace para "verificar" sus datos. El enlace lo lleva a una página web idéntica a la del banco, pero falsa, donde la víctima introduce sus credenciales, quedando entonces en poder del ciberdelincuente para su uso ilícito.[9]

- **Smishing:** similar al phishing, pero utilizando mensajes de texto (SMS). El término surge de la fusión de SMS y phishing.

    - Ejemplo: se recibe un SMS que dice: "su paquete se encuentra retenido por problemas con la dirección. Favor ingresar al enlace y actualizar sus datos"[10]. Al hacer clic, se pide información personal o se descarga un software malicioso.

- **Malware:** programa malicioso diseñado para infectar dispositivos, tomar control de ellos, extraer información confidencial u operar desde el dispositivo de la víctima.

    - Ejemplo: los enlaces o archivos que, al abrirlos, instalan un virus en la computadora que roba los datos bancarios del usuario o bloquea su sistema pidiendo un rescate.

  Como puede apreciarse, el malware tiene dos efectos: paralizar el sistema que no puede operarse si el ciberatacante no habilita los accesos (neutraliza el malware), y el segundo, consiste en que el propio malware va transmitiendo los datos de la víctima, logrando capturar sus credenciales o específicamente los datos concernientes a sus accesos en cuentas.

- **SIM Swapping:** el estafador engaña a la empresa de telefonía para tomar el control de la línea móvil de la víctima.

    - Ejemplo: un ciberdelincuente, con engaños, manipula a la compañía telefónica de su víctima para que le transfiera "su número" a una tarjeta SIM que él controla. Con ese número, puede interceptar códigos de verificación de dos factores y acceder a sus cuentas bancarias o redes sociales.

[8] Los ataques de ingeniería social manipulan a las personas para que compartan información, descarguen software, visiten sitios web que comprometan su seguridad personal u organizacional.
[9] ArCERT. "Recomendaciones para evitar ser víctima del phishing". Facultad de Ciencias Económicas UNLP. https://www.econo.unlp.edu.ar/detise/phishing-3923.
[10] Scotiabank México. "Ejemplos de smishing y cómo protegerte | Blog | Scotiabank México". Scotiabank México, 11 de enero de 2024. http://www.scotiabank.com.mx/blog/para-ti-ejemplos-smishing-y-como-protegerte.

- **Aplicaciones Falsas (Fake Apps**): aplicaciones diseñadas para parecer legítimas — imitando a bancos, comercios, servicios de delivery o redes sociales— pero en realidad son creadas para robar datos personales, instalar malware o tomar el control del dispositivo del usuario[11].

    - Ejemplo: bajar una app con colores o logotipos similares a los del banco, suponiendo que es la correcta, sin previamente cerciorarse en la página web oficial de la entidad financiera, cuál es la app que el banco pone a disposición de los usuarios. Al abrirla e ingresar las credenciales, la app las envía directamente a los ciberdelincuentes, dándoles acceso total de la cuenta bancaria.

Tácticas como el phishing, smishing y aplicaciones falsas, ponen en manifiesto la falta de conciencia, el exceso de confianza o la falta de mayor prudencia ante la necesidad de actuar con rapidez en la toma de decisiones. La neutralización de este tipo de delitos y sus efectos exige no solo políticas públicas adecuadas, sino también conductas preventivas y una ineludible conducta diligente e informada del consumidor.

V. MEDIDAS PARA NEUTRALIZAR LOS EFECTOS DE LOS CIBERATAQUES

5.1 Por parte del consumidor

Ante los ataques cibernéticos, el consumidor puede adoptar dos tipos de medidas: unas preventivas y otras reactivas. Las primeras se caracterizan por anticiparse, actuando con diligencia, sin haber recibido ningún ataque; las otras, también implican conductas diligentes, pero a raíz de la evidencia de un ataque.

Las medidas preventivas pueden consistir en el cuidado especial respecto de las credenciales; para mantenerlas seguras se suelen seleccionar contraseñas "fuertes" (difíciles de descifrar), por ejemplo: usar al menos 12 caracteres, combinando mayúsculas, minúsculas, números y símbolos, evitando repetir claves. Asimismo, es indispensable contar con un antivirus y antimalware activos y actualizados en los equipos con acceso a internet, que manejan datos sensibles o se conectan a redes compartidas y, en lo posible, evitar redes Wi-Fi públicas para transacciones; si ello fuera inevitable, sería recomendable incorporar el uso de VPN[12]. Verificar remitentes y URLs antes de acceder o descargar archivos y evitar compartir datos bancarios por teléfono, correo o redes. Configurar en el celular alertas en banca digital para movimientos y retiros.

Las medidas reactivas (adaptadas durante un ataque), requieren una respuesta inmediata por parte del usuario. Es decir, si se sospecha de alguna intrusión, se debe desconectar el dispositivo de internet y cambiar contraseñas desde un equipo seguro. En caso no sea posible, se debe efectuar una comunicación al banco de inmediato para bloquear cuentas o tarjetas y guardar evidencias (capturas de pantalla, mensajes, correos) para

[11] La República. "Usuaria denuncia estafa a través de supuesto aplicativo de Banco Pichincha: "Te vacían todas tus cuentas"". La República, 8 de mayo de 2024. https://larepublica.pe/economia/2024/05/04/usuaria-denuncia-estafa-a-traves-de-supuesto-aplicativo-de-banco-pichincha-te-vacian-todas-tus-cuentas-estafas-banco-financiero-atmp-247785.

[12] Red privada virtual (RPV, en inglés, *Virtual Private Network*-VPN). Es una tecnología de red que permite una extensión segura de la red de área local (LAN, por sus siglas en inglés Local Area Network) sobre una red pública o no controlada como Internet.

acreditar el ataque. Finalmente, debe contactarse (en Perú) a la División de Investigación de Delitos de Alta Tecnología – DIVINDAT PNP.

Luego del ataque, deberán tomarse medidas para neutralizar efectos residuales y evitar reincidencia, tales como solicitar nuevos medios de pago (tarjetas, tokens). El usuario deberá continuar monitoreando los estados de cuenta y reportar movimientos no reconocidos.

Finalmente, es importante que el consumidor mantenga buenas prácticas para evitar este tipo de situaciones, tales como la capacitación continua: mantenerse al día con alertas de la Superintendencia de Banca, Seguros y AFP (SBS), bancos y de la Policía Nacional del Perú (PNP). Guardar comprobantes y comunicaciones permite sustentar el eventual reclamo o denuncia ante el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) o ante la SBS.

5.2 Por parte del proveedor

De otro lado, es responsabilidad del proveedor ejecutar todas las medidas preventivas y reactivas posibles para evitar ciberataques. El proveedor debe mantener la seguridad de infraestructura y datos, implementando firewalls (controlan y filtran el tráfico de datos de una red o de un dispositivo), de acuerdo con reglas de seguridad predefinidas.

En esa línea, deben tener implementado un procedimiento de identificación idóneo. Para tal efecto, los proveedores deben mantener una capacitación y cultura de ciberseguridad, con un entrenamiento periódico a sus empleados en delitos cibernéticos y manejo de incidentes. Se debe contar con simulacros internos de ciberataques para evaluar la capacidad de respuesta, así como con protocolos o planes de recuperación ante desastres.

Como puede apreciarse, se trata de obligaciones de medios, por lo que cabe documentar las medidas preventivas (escenario antes del ataque) y las acciones concretas para limitar el impacto y reparar daños después del ataque. Todo ello en un tiempo oportuno para detectar y actuar.

Si no se actúa diligentemente "antes" y "después", los proveedores pueden terminar asumiendo la responsabilidad de las consecuencias de un ciberataque por falta de prevención y reacción.

5.2.1 Autenticación reforzada: asegurando la identificación del usuario

Como parte de las medidas preventivas para reducir el riesgo de ciberataques, resulta indispensable la aplicación de mecanismos de autenticación reforzada. Este proceso incrementa el nivel de seguridad al exigir la verificación mediante dos o más factores independientes y resistentes al fraude, lo que dificulta la suplantación de identidad del usuario legítimo.

En las plataformas digitales bancarias, un paso inicial clave es el enrolamiento: proceso mediante el cual el usuario registra y valida los factores de autenticación que quedarán asociados a su identidad, tales como credenciales, dispositivos, tokens o datos biométricos.

El enrolamiento constituye el punto de partida de la experiencia digital del cliente y debe realizarse bajo criterios de autenticación reforzada. Con ello, se asegura que el canal o dispositivo quede vinculado al titular desde el inicio, sentando las bases de un proceso de verificación confiable en todas las operaciones posteriores.

- **Autenticación de Doble Factor (2FA):**

Una vez que el usuario se haya enrolado al sistema de la entidad financiera, cuando desee realizar alguna transacción se le requerirán mecanismos de autenticación reforzada, que generalmente implica el uso de dos factores (2FA, por sus siglas en inglés Two-Factor Authentication). En este proceso, el usuario debe validar su identidad mediante la combinación de elementos de distinta naturaleza, tales como:

- **Algo que el usuario sabe**: información generalmente memorizada por el usuario, tales como una contraseña o un PIN.
- **Algo que el usuario tiene**: se trata de un dispositivo físico o medio al cual solo el usuario debería tener acceso. Por ejemplo, una clave dinámica, verificación por SMS, notificación push, entre otros.
- **Algo que el usuario es**: rasgos biométricos, como una huella digital, reconocimiento facial o reconocimiento de voz.

La autenticación de doble factor dificulta que los hackers accedan a las cuentas de sus víctimas y realicen transacciones. Hoy no basta con solo tener la contraseña del usuario; con la 2FA se requiere información adicional de identificación para que la operación sea correctamente procesada. Para entenderlo, a modo figurativo, la autenticación de doble factor sería como tener una segunda cerradura con una llave diferente antes de entrar a casa. Aunque el ladrón encuentre la primera llave, no podrá entrar sin la segunda.

VI. EL ANÁLISIS DEL INDECOPI EN LA VALIDACIÓN DE MEDIDAS DE SEGURIDAD

A lo largo de este artículo, hemos tratado la problemática de los delitos cibernéticos y el rol que juegan tanto consumidores como proveedores para prevenirlos. Sin perjuicio de ello, una vez que ocurren, el consumidor tiene la posibilidad de acudir a las autoridades correspondientes, en caso considere que la entidad bancaria descuidó su deber de diligencia; ya sea presentando denuncias, reclamos o demandas ante la SBS, el INDECOPI o el Poder Judicial, con el fin de generar una restitución de lo sustraído.

Como puede apreciarse, si bien el verdadero responsable en los ciberdelitos financieros es el delincuente, las partes que forman la relación de consumo (banco y consumidor), tienen también su propia responsabilidad. Si alguno incumple las medidas básicas de seguridad para evitar que estos hechos delictivos ocurran, lo que sucederá es que no podrá desplazar las consecuencias.

De ahí la importancia de adoptar medidas diligentemente, para así evitar que consumidor y proveedor asuman el detrimento económico causado por el ciberdelincuente. En esa línea, es preciso señalar que el ordenamiento legal no ha puesto a su cargo las mismas reglas o medidas de diligencia. Si estas no se adoptan o implementan, cada uno tendrá que asumir, según el caso, las consecuencias. Por un lado, si el banco no cumple con las medidas mínimas y tiene un sistema endeble, tendrá que responderle al consumidor por las vulneraciones a sus sistemas. De ese modo, se verifica que el proveedor habría expuesto culposamente el patrimonio del consumidor, al tener un sistema riesgoso y sin medidas que neutralicen el ataque a ciberdelincuentes. En ese escenario, se deberá corroborar si fue el banco quien mantuvo sistemas obsoletos e incumplió con su obligación de contar con las medidas de seguridad indispensables.

Por otro lado, cabe también la posibilidad de que haya sido el mismo consumidor quien no observó los parámetros mínimos para evitar el ciberataque, siendo negligente con el cuidado de sus contraseñas, empleando redes inseguras, abriendo enlaces de dudosa procedencia o no reportando oportunamente la pérdida/robo de sus tarjetas o celular

para que el banco tome las medidas inmediatas de bloqueo. En esos casos, la entidad financiera no tendría por qué asumir el detrimento patrimonial que hubiera podido sufrir el consumidor[13].

El INDECOPI ha jugado un papel crucial en la resolución de disputas referidas a la ciberseguridad en el consumo digital. Sus resoluciones ofrecen valiosas lecciones que permiten evidenciar el grado de responsabilidad, tanto de proveedores, como de consumidores. En efecto, para determinar la responsabilidad del proveedor en estas situaciones, el análisis del INDECOPI se centra en la correcta aplicación de medidas de seguridad desde dos frentes: el patrón de consumo y la validez de la operación.

6.1 Sobre el patrón de consumo

El Reglamento de Tarjetas de Crédito y Débito define al comportamiento habitual de consumo del usuario[14] como el tipo de operaciones usualmente realizadas, considerando diversos factores, entre ellos, el país de consumo, tipos de comercio, frecuencia, canal utilizado, etc.; los cuales pueden ser determinados a partir de la información histórica de las operaciones que cada usuario registre en la empresa.

Teniendo esto en cuenta, el comportamiento habitual del cliente es considerado un parámetro fundamental e indispensable en la resolución de controversias por operaciones no reconocidas en canales digitales. Por tanto, el patrón de consumo se estaría entendiendo, según el criterio del INDECOPI, como un tipo de "garantía legal" dentro del parámetro de idoneidad en la prestación de servicios y productos financieros, debiendo formar parte de las medidas de seguridad que las entidades financieras ofrecen a sus clientes, encontrándose entre ellas, el deber de monitoreo y detección de consumos inusuales o sospechosos.

En efecto, para la Sala Especializada en Protección al Consumidor del INDECOPI (en adelante, la Sala), la autoridad administrativa debe evaluar el cumplimiento de dicha "garantía legal", incluso aunque el consumidor no hubiera cuestionado su observancia de forma completa o explícita[15].

Bajo ese orden de ideas, la Sala ha fijado "parámetros" para otorgar un "criterio objetivo" que determine el comportamiento habitual del consumidor. Considera que se debe tomar en cuenta el importe individual de las operaciones que el consumidor usualmente realizó

---

[13] En este contexto, los seguros juegan un rol complementario, al trasladar los riesgos derivados de delitos cibernéticos hacia la empresa aseguradora, la cual asume el impacto económico y operativo de los daños. De esta forma, se atenúan las consecuencias directas sobre los consumidores y proveedores financieros, siempre que exista una adecuada evaluación de cobertura y responsabilidad compartida en la prevención.

[14] Perú. Superintendencia de Banca y Seguros - SBS. Reglamento de Tarjetas de Crédito y Débito. Resolución S.B.S. N° 6523-2013
Artículo 2°.- Definiciones Para efectos de lo dispuesto en el presente Reglamento, se considerarán las siguientes definiciones:
(…)
5. Comportamiento habitual de consumo del usuario: se refiere al tipo de operaciones que usualmente realiza cada usuario con sus tarjetas, considerando diversos factores, como por ejemplo el país de consumo, tipos de comercio, frecuencia, canal utilizado, entre otros, los cuales pueden ser determinados a partir de la información histórica de las operaciones de cada usuario que registra la empresa
(…)

[15] Considerando 41, INDECOPI. 21 de julio de 2025. Resolución N° 2304-2025/SPC-INDECOPI (Perú)

con el producto objeto de denuncia antes de la operación irregular. Esto se obtiene del estudio de los estados de cuenta de las líneas de crédito y/o cuentas denunciadas. De ese modo, para determinar si una operación es inusual o no al comportamiento habitual de consumo del cliente, la Sala considerará si, previamente, se realizaron operaciones por importes similares a los hechos denunciados.

En otras palabras, la Sala considera que, para determinar el comportamiento habitual de consumo de un usuario, deberá verificarse el monto individual de las operaciones previamente cargadas y cuántas operaciones por día efectuaba el consumidor, de tal manera que se pueda constatar si la operación cuestionada podría alertar la existencia de algún movimiento irregular, evidenciándose la relevancia del patrón de consumo en el análisis de responsabilidad del proveedor financiero.

Incluso, mediante Resolución Final N° 2305-2025/SPC-INDECOPI, la Sala precisó que, en aquellos casos donde la operación debió generar alertas por no encontrarse dentro del patrón de consumo, no sería necesario corroborar si dicha operación fue procesada válidamente. Es decir, para la Sala, el patrón de consumo pasaría a ser una suerte de "primer filtro", siendo que el solo hecho de no haber detectado la irregularidad en el patrón habitual del consumidor, sería suficiente para determinar su responsabilidad. Por el contrario, si esta operación estuviera acorde a su comportamiento habitual de consumo, la responsabilidad del proveedor dependerá del análisis sobre el cumplimiento de los requisitos de validez de la operación para su autorización.

6.2 Sobre la validez de la operación

El criterio adoptado por la Sala en la Resolución 2293-2024/SPC del 19 de agosto de 2024, refiere a que las entidades financieras requieran contar con mecanismos tecnológicos suficientes para garantizar que todas las operaciones que vayan a procesar se hayan realizado de forma correcta. Es decir, que dichas operaciones deban encontrarse dentro de su comportamiento habitual de consumo y hayan sido autorizadas con los mecanismos de validez necesarios para cada tipo de transacción.

Sobre este último punto, la SBS emitió la Resolución SBS N° 504-2021, que aprobó el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, con la finalidad de que las entidades financieras fortalezcan sus capacidades de autenticación en el procesamiento de operaciones. Precisamente, en su artículo 19°, se prevén los requisitos de validez en las transacciones, tales como la necesidad de aplicar la autenticación reforzada[16] para aquellas acciones que puedan originar operaciones fraudulentas en perjuicio del cliente. Tenemos entonces que, para la realización de

[16] Perú. Superintendencia de Banca y Seguros - SBS. Reglamento de Ciberseguridad. Resolución S.B.S. N° 504-2021.
Artículo 19. Autenticación reforzada para operaciones por canal digital: Se requiere de autenticación reforzada para aquellas acciones que puedan originar operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente, como las operaciones a través de un canal digital que impliquen pagos o transferencia de fondos a terceros, registro de un beneficiario de confianza, modificación en los productos de seguro ahorro/inversión contratados, la contratación de un producto o servicio, modificación de límites y condiciones, para lo cual se requiere: a) Utilizar una combinación de factores de autenticación, según el literal j) del artículo 2 del presente Reglamento que, por lo menos, correspondan a dos categorías distintas y que sean independientes uno del otro. b) Generar un código de autenticación mediante métodos criptográficos, a partir de los datos específicos de cada operación, el cual debe utilizarse por única vez. c) Cuando la operación sea exitosa, notificar los datos de la operación al usuario.

operaciones a través de un canal digital, entre ellas, las transferencias de fondos a terceros, resulta de necesaria aplicación la autenticación reforzada:

i) Utilizar una combinación de factores de autenticación que correspondan a dos categorías distintas y que sean independientes uno del otro.
ii) Generar un código de autenticación mediante métodos criptográficos.
iii) Cuando la operación sea exitosa, notificar los datos de la operación al usuario.

En atención a ello, para INDECOPI resulta indispensable que, en el marco de un procedimiento administrativo, la entidad financiera acredite la realización de estos "tres pasos" para que la operación por canales digitales sea considerada como válidamente procesada y la responsabilidad no recaiga sobre ella.

VII. DISCREPANCIAS ENTTRE LA SBS Y EL INDECOPI

Existe una situación compleja, a raíz de la discrepancia significativa entre la SBS y el INDECOPI, respecto a cómo se determina la responsabilidad del proveedor en los casos de operaciones no reconocidas por canal digital.

Por un lado, la SBS establece que son las entidades financieras las que deben conocer a profundidad a sus clientes, determinando ellas mismas los parámetros y el perfil de patrón de consumo. Si bien ha precisado que, las entidades bajo su supervisión están obligadas a implementar sistemas de monitoreo para garantizar la seguridad en las operaciones con tarjetas (según el artículo 17 del Reglamento de Tarjetas de Crédito y Débito), no ha establecido ningún criterio, protocolo o definición específica, que permita a las empresas del sistema financiero categorizar una operación dentro de un patrón de consumo habitual. De ese modo, son las entidades financieras las únicas encargadas de fijar los parámetros del patrón de consumo que aplicarán. Ello les permitiría conocer mejor a su cliente, diseñar medidas preventivas, pero no considera que dicho patrón deba ser un mecanismo de seguridad que gatille responsabilidades para el Banco; pues los patrones de consumo no son fijos ni invariables. Por lo tanto, la SBS no considera al "patrón de consumo" como un elemento determinante para atribuir responsabilidad frente a operaciones no reconocidas.

En efecto, para determinar la responsabilidad de las entidades financieras en las operaciones no reconocidas por canal digital, el énfasis de la SBS únicamente radica en la "autenticación reforzada", sin definir claramente las implicancias del "patrón de consumo". Sugiere un enfoque regulatorio más centrado en la tecnología y menos en el comportamiento. La SBS considera que la "autenticación reforzada" por sí sola es suficiente, siempre que se cumplan los pasos técnicos establecidos, por lo que la responsabilidad del banco se considerará cumplida. Sin embargo, esto crea un posible punto ciego para las anomalías de comportamiento que podrían indicar fraude, incluso cuando la autenticación parezca técnicamente sólida, dejando a los consumidores vulnerables ante ataques sofisticados de ingeniería social.

De otro lado, el INDECOPI considera que se puede crear un patrón de consumo referencial, en base al registro histórico del usuario. Cabe señalar que este "patrón" creado, no tiene ningún respaldo legislativo ni técnico. Incluso en muchas Resoluciones este "patrón" de referencia cambia; es decir, en algunos casos se considera que el patrón deberá evaluarse considerando el promedio de consumos máximos efectuados en los 6 meses anteriores a las operaciones no reconocidas y, en otros casos, se toma como referencia los 12 meses. En algunos casos se considera que deben sumarse los consumos totales de cada mes para

sacar un promedio de "consumo mayor"; mientras que, en otros, se toma como punto de quiebre a la operación más alta de los meses evaluados, lo cual acusa de una severa debilidad, establecida en criterios administrativos que afectan la tipicidad y legalidad del cargo imputado. No obstante, para el INDECOPI esta información siempre puede permitir al banco determinar la existencia de alguna irregularidad y, de no hacerlo, debe encontrársele responsable.

Frente a este escenario, urge avanzar hacia una coordinación más estrecha entre la SBS (el órgano regulador de los bancas y operaciones) e INDECOPI (agencia de protección del consumidor), que permita la emisión de lineamientos conjuntos, protocolos de actuación estandarizados y criterios comunes para la interpretación del "patrón de consumo".

VIII. REFLEXIÓN FINAL: UN FUTURO DIGITAL MÁS SEGURO PARA TODOS

La ciberseguridad en el consumo digital es, sin duda, uno de los desafíos más apremiantes de nuestra era. Hemos visto cómo la digitalización ha transformado el riesgo de ser una amenaza localizada y limitada a un peligro masivo que puede afectar a millones en segundos desde cualquier parte del mundo. Las motivaciones detrás de los ataques son diversas, y las vulnerabilidades no solo provienen de actividades dolosas, sino también de la obsolescencia tecnológica, eventos imprevistos e inevitables y, crucialmente, de las fallas humanas.

A lo largo de este análisis, se ha puesto de manifiesto que la seguridad digital es una responsabilidad compartida. Los proveedores, especialmente las entidades financieras, tienen el deber de implementar y mantener mecanismos de seguridad robustos, como la autenticación de doble factor y la validación biométrica. La jurisprudencia de INDECOPI ha subrayado esta responsabilidad, exigiendo a los bancos no solo la existencia de estos mecanismos, sino la capacidad de probar su correcta activación y el cumplimiento de los protocolos de notificación. Este enfoque de INDECOPI, que ha evolucionado hacia un monitoreo preventivo del "patrón de consumo", contrasta con la postura de la SBS, que prioriza la autenticación reforzada como criterio principal. Esta divergencia destaca la necesidad de una vigilancia constante y una adaptación continua por parte de todos los actores.

La naturaleza dinámica de las ciber amenazas, con la constante aparición de nuevos tipos de fraude y la evolución de las tácticas de los atacantes, implica que las soluciones estáticas resultan insuficientes. Incluso los organismos reguladores están en un proceso de adaptación. Por lo tanto, la ciberseguridad requiere de una constante y continua actualización.

Para el consumidor, los cambios tecnológicos le recuerdan que la diligencia ordinaria debe estar presente en sus acciones, pues tienen que adaptarse al nuevo entorno y circunstancias en las relaciones de consumo digital. La diligencia personal, la adopción de contraseñas fuertes y únicas, la gestión inteligente de correos electrónicos, la precaución al navegar y descargar archivos, y la activación de la autenticación de doble factor son medidas sencillas pero poderosas. El conocimiento de los riesgos comunes, como los delitos cibernéticos, y la capacidad de reconocer las señales de alerta son herramientas invaluables para protegerse.

En última instancia, un futuro digital más seguro para todos depende de la colaboración. Proveedores y consumidores deben permanecer vigilantes, adaptarse a las nuevas amenazas y mejorar continuamente sus prácticas de seguridad. El conocimiento compartido y las medidas proactivas son el camino hacia un entorno digital donde la

confianza y la seguridad sean la norma, permitiéndonos disfrutar plenamente de los beneficios del consumo digital.

BIBLIOGRAFÍA

- ARCERT, "Recomendaciones para evitar ser víctima del phishing", Facultad de Ciencias Económicas UNLP, https://www.econo.unlp.edu.ar/detise/phishing-3923.
- Freddy Chávarry, "Fraudes digitales y suplantación de identidad: expertos analizan cifras de la PNP sobre impacto de la ciberdelincuencia", RPP Noticias, 3 de marzo de 2025, https://rpp.pe/peru/actualidad/fraudes-digitales-y-suplantacion-de-identidad-expertos-analizan-cifras-de-la-pnp-sobre-impacto-de-la-ciberdelincuencia-noticia-1620813.
- INDECOPI, 21 de julio de 2025, Resolución N° 2304-2025/SPC-INDECOPI (Perú).
- La República, "Usuaria denuncia estafa a través de supuesto aplicativo de Banco Pichincha: "Te vacían todas tus cuentas"", La República, 8 de mayo de 2024, https://larepublica.pe/economia/2024/05/04/usuaria-denuncia-estafa-a-traves-de-supuesto-aplicativo-de-banco-pichincha-te-vacian-todas-tus-cuentas-estafas-banco-financiero-atmp-247785.
- Martín Cifuentes, "¿El fin del dinero en efectivo? Sólo un 12% de los chilenos lo usa para pagar", La Tercera, 23 de agosto de 2023, https://www.latercera.com/piensa-digital/noticia/el-fin-del-dinero-en-efectivo-solo-un-12-de-los-chilenos-lo-usa-para-pagar/IAPJQA6BS5EZXFQ6PNYAZQOPA4.
- Matthew Kosinski et al., "¿Qué es la autenticación de dos factores (2FA)?", IBM, 24 de mayo de 2025, https://www.ibm.com/es-es/think/topics/2fa.
- Pablo Verderas et al., "Estudio Medios de Pago en el Perú 2025", NTT DATA, 2025, https://pe.nttdata.com/documents/NTT%20DATA%20-%20PAYMENT.pdf.
- Perú, Superintendencia de Banca y Seguros - SBS, Reglamento de Ciberseguridad, Resolución S.B.S. N° 504-2021
- Perú, Superintendencia de Banca y Seguros - SBS, Reglamento de Tarjetas de Crédito y Débito, Resolución S.B.S. N° 6523-2013
- Scotiabank México, "Ejemplos de smishing y cómo protegerte | Blog | Scotiabank México", Scotiabank México, 11 de enero de 2024, http://www.scotiabank.com.mx/blog/para-ti-ejemplos-smishing-y-como-protegerte.
- SOTESA, "Consejos de ciberseguridad para proteger tus equipos", Sotesa, https://sotesa.com/consejos-de-ciberseguridad/.