Proyecto de Ley N° 3251/2022 - CR

CONGRESO de la REPÚBLICA

MARÍA ELIZABETH TAIPE CORONADO
Congresista de la República

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"
"Año del Bicentenario del Congreso de la República del Perú"

PROYECTO DE LEY _____

CONGRESO DE LA REPÚBLICA
Área de Trámite y Digitalización de Documentos
10 OCT. 2022
RECIBIDO
Firma _____ Hora 3:40 p.m.

PROYECTO DE LEY QUE REGULA LA RESPONSABILIDAD DE LAS EMPRESAS DEL SISTEMA FINANCIERO ANTE EL FRAUDE INFORMÁTICO PARA LA PROTECCIÓN DE LOS CONSUMIDORES

El Grupo Parlamentario **PERÚ LIBRE** a iniciativa de la Congresista **MARÍA ELIZABETH TAIPE CORONADO** y de los congresistas firmantes, ejerciendo el derecho a iniciativa legislativa que les confiere el artículo 107 de la Constitución Política del Perú, y en concordancia con los artículos 22, inciso c), 67, 75 y 76 del Reglamento del Congreso de la República, presentan el siguiente proyecto de ley:

FÓRMULA LEGAL

EL CONGRESO DE LA REPÚBLICA
Ha dado la siguiente Ley:

PROYECTO DE LEY QUE REGULA LA RESPONSABILIDAD DE LAS EMPRESAS DEL SISTEMA FINANCIERO ANTE EL FRAUDE INFORMÁTICO PARA LA PROTECCIÓN DE LOS CONSUMIDORES

Artículo 1.- Objeto
La presente ley tiene por objeto regular la responsabilidad de las empresas del Sistema Financiero, respecto de los fraudes informáticos cometidos contra los usuarios de este sistema ante operaciones activas y pasivas fraudulentas, estableciendo las acciones que deberán asumir y determinar los tiempos para la resolución de los casos.

Artículo 2.- Finalidad
La ley tiene por finalidad proteger y garantizar las operaciones activas y pasivas que realizan los usuarios del sistema financiero, reduciendo el perjuicio económico y salvaguardar la buena reputación crediticia.

Artículo 3.- Ámbito de aplicación
La ley es aplicable a todas las empresas que operan en el sistema financiero.

Artículo 4.- Incorporación
Se incorpora el subcapítulo IV, al Título III, de la Sección Segunda de la Ley 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, en los siguientes términos:

SUBCAPÍTULO IV
FRAUDE INFORMÁTICO

Artículo 281-A. Obligaciones
Del usuario

a) Utilizará el instrumento y canales virtuales de pago de conformidad con las condiciones reguladas por la Superintendencia de Banca, Seguros y AFP.

b) Deberá informar a la empresa financiera en caso de pérdida, hurto, robo o apropiación indebida del instrumento de pago, en el más breve plazo de ocurrido el hecho o que se haya tomado conocimiento del mismo.
c) Preverá las medidas de protección y salvaguarda del instrumento de pago, así como las claves de seguridad generadas y datos personales.

De las empresas del sistema financiero

a) Deberá implementar los mecanismos de la más alta tecnología para proteger las operaciones activas y pasivas, las claves generadas y los datos personales del usuario, asegurando que solo el usuario tenga acceso a dicha información.
b) Solo en caso que el usuario solicite la sustitución del instrumento de pago, la empresa emitirá uno nuevo, en ningún caso emitirá un instrumento de pago que no haya sido solicitado expresamente por el usuario.
c) Deberá asegurar que sus canales de atención remota estén disponibles las 24 horas del día, los 7 días de la semana, incluyendo feriados y días no laborables, para que el usuario pueda reportar la pérdida, hurto, robo o clonación del instrumento de pago u operaciones no autorizadas; respecto de sus medios de atención presencial estos deberán priorizar la atención del usuario que requiera notificar alguna de las situaciones mencionadas.
d) Los reportes a los que se refiere el literal c) no deberán irrogarle ningún gasto adicional al usuario, salvo los referidos a la reposición del instrumento de pago de ser el caso.
e) Una vez notificado el hecho que genere el bloqueo del instrumento de pago, la empresa imposibilitará la utilización del mismo en todas las modalidades de uso (cajeros, plataformas virtuales, banca móvil, proveedores de servicios de pago).

Artículo 281-B. Responsabilidad de la empresa en caso de operaciones no autorizadas

1. Ante una operación no autorizada, la empresa deberá devolver el importe de esta operación de inmediato y, en cualquier caso, a más tardar al siguiente día hábil de reportado el incidente.
2. Ante operaciones activas (préstamos, créditos, etc.) no autorizadas, la empresa deberá anular esta operación, sin causar perjuicio en la reputación crediticia del usuario, a más tardar al siguiente día hábil de reportado el incidente.
3. En los casos en que la empresa tenga indicios razonales para dudar de la veracidad del reporte de la operación (activa o pasiva) no autorizada, deberá informar por escrito, en los mismos plazos, a la Superintendencia de Banca, Seguros y AFP, así como al usuario, adjuntado los medios probatorios que sustentan su posición.
4. La empresa, en los casos mencionados, deberá restituir las cuentas bancarias, que hayan sido vulneradas, o los historiales crediticios al estado anterior al que se encontraba de no haberse realizado la operación no autorizada.
5. Cuando la operación no autorizada se haya realizado a través de plataforma o página web distinta a la de la empresa bancaria, será esta última quien devolverá el importe de esta operación de inmediato, en cualquier caso, a más tardar al siguiente día hábil de reportado el incidente.

Artículo 281-C. Verificación de las operaciones no autorizadas

1. Cuando un usuario niegue haber autorizado una operación, corresponderá a la empresa demostrar que para dicha operación se activaron todos los mecanismos de verificación que demuestren que dicha operación fue correctamente registrada y que no se vio afectada por alguna falla de sistema. Esta verificación deberá realizarse a más tardas al día siguiente hábil de reportado el incidente, para dar cumplimiento a lo dispuesto en el numeral 1 del artículo 281-B.
2. Cuando un usuario niegue haber autorizado una operación, la sola utilización del instrumento, no bastará para demostrar que dicha operación ha sido autorizada por el usuario, ni que este ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave u omisión de sus obligaciones.
3. La empresa, aportará pruebas para demostrar, de ser el caso, que el usuario hubiera cometido fraude o negligencia grave.

DISPOSICIONES COMPLEMENTARIA FINAL

ÚNICA. Adecuación de la reglamentación

Se encarga a la Superintendencia de Banca, Seguros y AFP, para que en el plazo de sesenta (60) días calendario, adecue los reglamentos de la materia a lo previsto en la presente Ley.

FIRMA DIGITAL
Firmado digitalmente por: QUITO SARMIENTO Bernardo Jaime FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 10/10/2022 13:50:48-0500

MARÍA ELIZABETH TAIPE CORONADO
Congresista de la República del Perú

FIRMA DIGITAL
Firmado digitalmente por: PORTALATINO AVALOS Kelly Roxana FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 10/10/2022 10:50:37-0500

FIRMA DIGITAL
Firmado digitalmente por: TAIPE CORONADO Maria Elizabeth FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 04/10/2022 10:54:56-0500

FIRMA DIGITAL
Firmado digitalmente por: GONZA CASTILLO Américo FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 06/10/2022 21:05:01-0500

FIRMA DIGITAL
Firmado digitalmente por: PARIONA SINCHE Alfredo FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 06/10/2022 15:29:14-0500

FIRMA DIGITAL
Firmado digitalmente por: PORTALATINO AVALOS Kelly Roxana FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 10/10/2022 10:50:51-0500

FIRMA DIGITAL
Firmado digitalmente por: QUISPE MAMANI Wilson Rusbel FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 10/10/2022 12:53:12-0500

EXPOSICIÓN DE MOTIVOS

1. Fundamentación

La presente iniciativa legislativa busca regular la responsabilidad de las empresas del Sistema Financiero ante el fraude cibernético con la finalidad de proteger los derechos de los usuarios, quienes están siendo víctimas de esta clase de delitos en razón al auge de la tecnología.

Es una realidad que con la llegada del internet los tiempos han cambiado, hace algunos años atrás la única opción para realizar transacciones (pagos, cobros, giros, etc.) era apersonarse a la entidad financiera y realizar dicha gestión, sin embargo, con el avance de la tecnología y la implementación de mecanismos remotos para realizar operaciones esta realidad ha cambiado, si bien es cierto, es un beneficio para los usuarios en la medida que se ahorra tiempo, dinero, teniendo a disposición los canales de atención, en su mayoría, las 24 horas.

Respecto al uso del Internet enfocado específicamente a América Latina y El Caribe, el Banco Interamericano de Desarrollo – BID[1] precisa lo siguiente:

> La realidad contundente de nuestro tiempo es que el Internet ha revolucionado la forma en que interactuamos con los demás y el mundo que nos rodea. El aumento de la conectividad a Internet hace que un número cada vez mayor de personas estén conectadas en un espacio en gran parte público y transnacional, y proporciona una plataforma dinámica y de crecimiento que permite que avance la comunicación, la colaboración y la innovación en maneras en que nunca hubiéramos podido imaginar hace muy poco tiempo. Esto es particularmente cierto en América Latina y el Caribe, donde más de la mitad de nuestra población ya está en línea y la tasa de crecimiento de usuarios de Internet se encuentra entre las más altas del mundo. En las Américas y el Caribe estamos utilizando el Internet para compartir ideas y cultura; para mejorar el gobierno y los servicios sociales; para colaborar en la educación, las ciencias y las artes; y para hacer negocios, todo con una mayor accesibilidad y eficiencia. Los mayores beneficios de este nuevo paradigma que está emergiendo rápidamente es el impacto que ha tenido en la estimulación de un nuevo crecimiento y desarrollo social y económico de la región.

Como contraparte tenemos la aparición, expansión y desarrollo de la ciberdelincuencia, la que le cuesta al mundo al mundo US$575.000 millones al año[2], nuestro país no es ajeno a esta situación según la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) entre enero a diciembre de 2021 recibieron 1188 denuncias referidas a delitos cibernéticos[3].

Según informe de la ONU[4] "el cardin, por el que las organizaciones criminales utilizaban la información confidencial de las tarjetas bancarias para realizar compras por Internet" es una de las principales modalidades de fraude

---

[1] BID (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?
[2] Center for Strategic and International Studies and McAfee. Net Losses: Estimating the Global Cost of Cybercrime
[3] Diario El Peruano. Setiembre 2022. Ciberdelitos en el Perú: se elevan denuncias de fraude informático y suplantación de identidad.
[4] Lucha contra la de la información y las comunicaciones con fines delictivos.

informático en nuestro país. Actualmente, existen diversas modalidades empleadas por los ciberdelincuentes para obtener información privada como el phishing, la oferta de productos a muy bajo costo que llama la atención de los clientes pero que se realizan a través de páginas falsas o que no existen, así como la suplantación en redes sociales y aplicativos de comunicación instantánea.

Uno de los factores que abrió las puertas a la ciberdelincuencia fue la llegada de la pandemia generada por la Covid-19, según el Ministerio de Salud, en el Perú, el primer caso se registró en marzo de 2020 a partir de esta fecha el avance de los contagios fueron incrementado de manera exponencial, en ese escenario y, con la finalidad de reducir el riesgo de contagio y proteger la salud de los peruanos, el gobierno de turno, mediante Decreto Supremo Nº 044-2020-PCM, decretó el Estado de Emergencia Nacional, y dispuso el aislamiento social obligatorio (cuarentena), por las graves circunstancias que afectaban la vida de la Nación a consecuencia del brote del COVID-19[5], siendo ello así, los ciudadanos nos tuvimos que adaptar a nuevas formas de realizar trámites, compras, trabajo, entre otros, en la medida que no podíamos desplazarnos con total libertad, la tecnología fue de gran apoyo, según Charles Caillaux Caillaux en su artículo "¿Cuánto ha transformado la tecnología nuestras vidas durante la pandemia?[6]" precisa lo siguiente:

> El 2020 marcó un hito en el aumento del uso de plataformas y herramientas tecnológicas, con un aumento de 70 % a 300 %, según las actividades realizadas a diario. Se evidenció un crecimiento exponencial en aplicaciones de e-commercey pagos online, para comprar víveres; la telemedicina, para atender consultas de salud remotas, y el teletrabajo, para mantener las tareas laborales desde casa.

En esa línea, nos vimos obligados a usar medios remotos de atención, hecho que generó el incremento del fraude cibernético, asímismo los usuarios del sistema financiero hicimos mayor uso de las tarjetas de crédito y débito, con la finalidad de realizar compras, pagar servicios, entre otros, según el Ministerio Público en los últimos años a nivel nacional se registraron 21,687 denuncias por delitos informáticos incrementándose esta estadística durante la emergencia sanitaria[7].

1.1. Mecanismos utilizados por los ciberdelincuentes

Según el Banco Central de Reserva del Perú, en su publicación Medidas de Seguridad en las Tarjetas de Crédito[8], para el año 2015 en nuestro país, el uso de tarjetas de crédito se incrementó, de julio de 2015 respecto a julio de 2010 creció 30,7%, alcanzando los 8,0 millones; el manejo de este instrumento se puede dar en los mismos establecimientos de pago, cajeros automáticos, internet y a través de los aplicativos móviles, esta diversidad de canales ha dado lugar a las

[5] Decreto Supremo que declara Estado de Emergencia Nacional por las graves circunstancias que afectan la vida de la Nación a consecuencia del brote del COVID-19 – DS Nº 044-2020-PCM
[6] ESAN Graduate School of Business. ¿Cuánto ha transformado la tecnología nuestras vidas durante la pandemia? -
[7] Plataforma digital única del Estado peruano. Ministerio Público registró más de 21 mil denuncias por delitos informáticos en los últimos años. https://bit.ly/3RubauR
[8] Banco Central de Reserva del Perú. Medidas de Seguridad en las Tarjetas de Crédito. https://bit.ly/3fmMgj6

transacciones fraudulentas, en esta misma publicación se describe las principales modalidades de la siguiente manera:

a) Clonación o *skimming*, con un *skimmer*, al realizar una transacción desde un punto de venta o un cajero automático se roban datos de la banda magnética de la tarjeta y con esa información se genera una tarjeta falsa. Para concretar el fraude también se debe falsificarla firma del usuario.

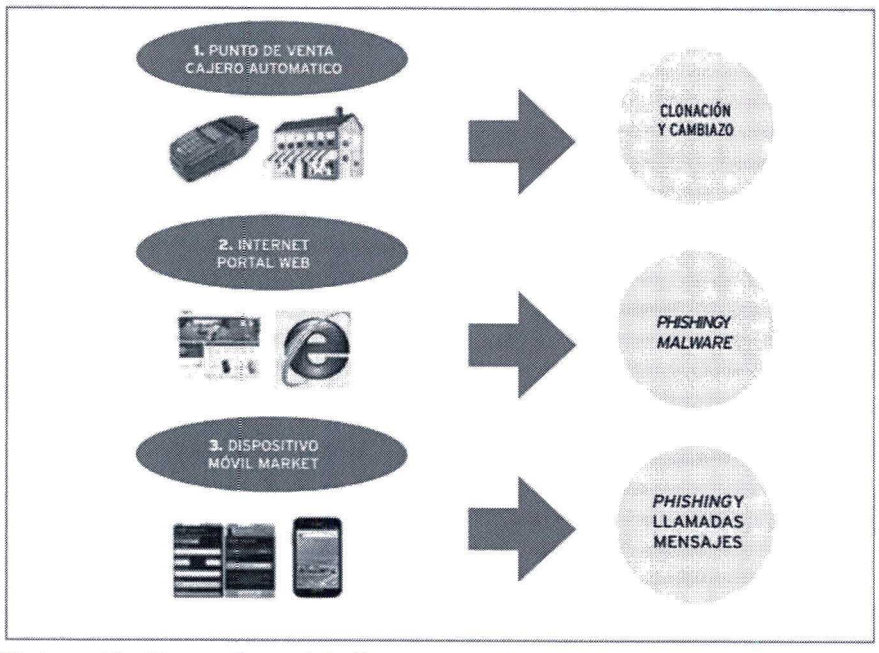
b) Cambiazo, un tercero, cambia o roba la tarjeta cuya clave ha observado y con ello realiza retiros de dinero desde cajeros automáticos a nombre del usuario.

c) *Phishing*, se envían correos con enlaces a páginas web falsas, usando el nombre de entidades financieras, para obtener datos personales y de la tarjeta. Las modalidades de *phishing* son: (1) páginas web, (2) formularios de correo electrónico y (3) redes sociales.

d) Malware, programa que se instala en la computadora del usuario, extrae sus datos y los envía automáticamente. Por lo general, se accede a estos programas desde páginas web vinculadas en correos falsos. Los principales tipos de malware son: (1) gusano, (2) virus y (3) troyano.

e) Llamadas y mensajes, el fraude a través de llamadas telefónicas se denomina *vishing* y por mensajes de texto *smishing*. Consiste en contactar al usuario para obtener datos personales y de la tarjeta.

En el cuadro que se presenta a continuación, elaborado por el BCRP, se puede observar los tipos de fraudes asociados a los canales de uso de las tarjetas de crédito y para efectos de este análisis aplicable también a las tarjetas de débito:



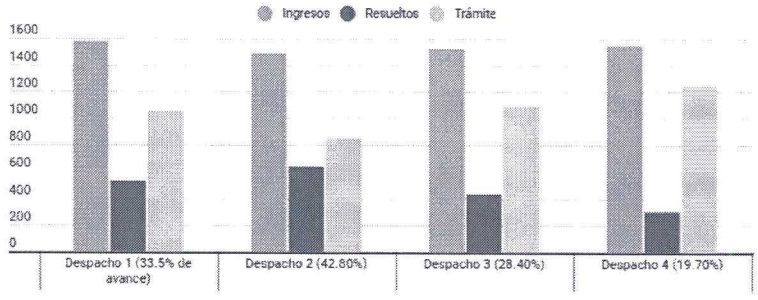
Elaboración: Banco Central de Reserva del Perú

1.2. Estadísticas de fraudes cibernéticos

1.2.1. Ministerio Público

En diciembre de 2020 el Ministerio Público creó la Unidad Fiscal Especializada en Ciberdelincuencia, creada con la finalidad de brindar acompañamiento técnico a los fiscales que investigan estos casos. La Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro (fiscalía que tiene la mayor cantidad de delitos investigados) reportó que entre enero y abril de 2022 han recibido 6,138 casos, de los cuales 1,903 ya fueron resueltos, según información recibida por la Agencia Peruana de Noticias Andina[9].

Casos ingresados, resueltos y en trámite en la Fiscalía Especializada en Ciberdelincuencia (Lima Centro)

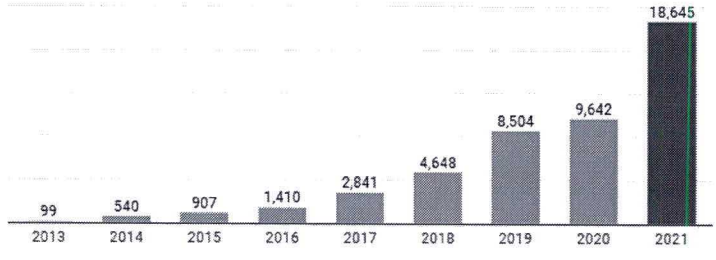


Fuente: Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público (enero a abril 2022)

andina

Respecto a la cantidad de denuncias ingresadas al Ministerio Público por delitos informáticos, la Unidad Fiscal Especializada en Ciberdelincuencia reportó las siguientes cifras[10]:

Delitos informáticos ley N° 30096 registrados en el Ministerio Público a escala nacional
Período 2013 al 2021



Fuente: Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público

andina

[9] Agencia Peruana de Noticias Andina. Conoce cómo trabajan los fiscales peruanos que investigan delitos de ciberdelincuencia. https://bit.ly/3E6mt9v
[10] Ídem

1.2.2. Instituto Nacional de Estadísticas e Informática - INEI

Esta institución del Estado, todos los años emite el informe técnico "Estadísticas de Criminalidad, Seguridad Ciudadana y Violencia" el mismo que tiene información proporcionada por el Ministerio del Interior a través de la Policía Nacional del Perú.

El pasado junio (2022) emitieron dicho informe del periodo comprendido entre enero a marzo de este año, el que contiene la data de los delitos informáticos, precisa además que en razón al auge de la tecnología este tipo de delitos deben de tener su propia estadística, siendo ello así informa lo siguiente[11]:

> En los meses de octubre a diciembre 2021, a nivel nacional, se registraron 391 denuncias por delitos informáticos, cifra mayor en 21 casos (5,7%) al compararse con similar periodo 2020.
> El mayor número de denuncias por comisión de delitos informáticos registrados en este periodo se observó en Lima Metropolitana (150), seguido por Lambayeque (34) y La Libertad (30). En el otro extremo, Ayacucho presentó solo un (1) caso por este tipo de delito.
> Cabe resaltar el crecimiento porcentual significativo de denuncias por delitos informáticos en algunos departamentos como Cajamarca, Departamento de Lima, Ica, Amazonas, Moquegua, San Martín y Puno (superior al 100%).

En el siguiente cuadro (del mismo informe) el INEI presenta las denuncias por comisión de delitos informáticos, según departamento entre octubre – diciembre, 2019 – 2021:

CUADRO Nº 1.4
Perú: Denuncias por comisión de delitos informáticos, según departamento
Octubre - Diciembre, 2019 - 2021

Departamento	2019 Oct - Dic	2020 Oct - Dic	2021 Oct - Dic	Variación 2021 / 2019		Variación 2021 / 2020	
				Absoluta	%	Absoluta	%
Total	316	370	391	75	23,7	21	5,7
Amazonas	6	2	5	-1	-16,7	3	150,0
Áncash	25	18	21	-5	-19,2	3	16,7
Apurímac	-	-	3	3	-	3	-
Arequipa	8	19	11	3	37,5	-8	-42,1
Ayacucho	1	7	1	0	0,0	-6	-85,7
Cajamarca	3	1	6	3	100,0	5	500,0
Prov. Const. del Callao	11	20	8	-3	-27,3	-12	-60,0
Cusco	15	27	11	-4	-26,7	-16	-59,3
Huancavelica	1	4	3	2	200,0	-1	-25,0
Huánuco	8	20	10	2	25,0	-10	-50,0
Ica	5	5	17	12	240,0	12	240,0
Junín	5	28	16	11	220,0	-12	-42,9
La Libertad	25	21	30	5	20,0	9	42,9
Lambayeque	17	32	34	17	100,0	2	6,3
Lima Metropolitana 1/	156	115	150	-6	-3,8	35	30,4
Departamento de Lima 2/	2	3	12	10	500,0	9	300,0
Loreto	1	4	3	2	200,0	-1	-25,0
Madre de Dios	-	-	9	9	-	9	-
Moquegua	5	2	5	0	0,0	3	150,0
Pasco	-	6	-	0	0,0	-6	-100,0
Piura	6	13	10	4	66,7	-3	-23,1
Puno	5	3	7	2	40,0	4	133,3
San Martín	1	2	5	4	400,0	3	150,0
Tacna	1	6	6	5	500,0	0	0,0
Tumbes	2	2	2	0	0,0	0	0,0
Ucayali	6	10	6	0	0,0	-4	-40,0

1/ Denominación establecida mediante Ley N° 31140, comprende los 43 distritos de la provincia de Lima.
2/ Denominación establecida mediante Ley N° 31140, constituido por las provincias de Barranca, Cajatambo, Canta, Cañete, Huaral, Huarochirí, Huaura, Oyón y Yauyos.
Fuente: Ministerio del Interior - Sistema de Denuncias Policiales-SIDPOL.
Elaboración: Instituto Nacional de Estadística e Informática.

[11] Informe Técnico N° 3 – junio 2022. Estadísticas de Criminalidad, Seguridad Ciudadana y Violencia. Una visión desde los registros administrativos. https://bit.ly/3UHuFTc

1.2.3 Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI

El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI, sobre el tema materia de exposición, a través de su Informe Anual sobre el Estado de la Protección de los Consumidores en el Perú – 2020 indica que del total de los reclamos resueltos en el 2020 uno de los motivos con mayor incidencia fueron los referidos a las operaciones no reconocidas, representando el 16.90% del universo, precisando además que 64.8% de reclamos resueltos versaron sobre tarjetas de crédito y cuentas de ahorro, en el siguiente gráfico[12] INDECOPI muestra los motivos de reclamos que ha recibido y que fueran resueltos en el 2020:

Tabla N° 75

Reclamos resueltos por las empresas 2020, según motivo de reclamo

Sistema	Motivo de reclamo	N° de reclamos 2020	Part. % 2020
Financiero	Cobros indebidos de intereses, comisiones, gastos y tributos (tales como seguros, ITF, etc., según corresponda)	1,060,276	35.82%
	Operaciones no reconocidas (consumos, disposiciones, retiros, cargos, abonos y sobregiros, según corresponda)	499,018	16.86%
	Transacciones no procesadas / mal realizadas	446,197	15.07%
	Inadecuada atención al usuario - Problemas en la calidad del servicio	147,611	4.99%
	Problemas con cajeros automáticos de titularidad u operados por la empresa (no dispensó efectivo o voucher, retención de tarjeta)	126,812	4.28%
	Fallas del sistema informático que dificultan operaciones y servicios	112,718	3.81%
	Inadecuada o insuficiente información sobre operaciones, productos y servicios	111,162	3.75%
	Otros	456,582	15.42%

1.2.4 Organismo Supervisor de la Inversión Privada en Telecomunicaciones – OSIPTEL

Como se ha explicado en párrafos anteriores, el fraude cibernético implica también el uso de aplicativos móviles, ante el robo, hurto o pérdida de un dispositivo móvil el usuario queda expuesto a ser víctima de alguna modalidad de fraude cibernético, para abril de 2022 OSIPTEL registró 132 990 reportes por robo de equipos[13], haciendo un promedio de más de 4 mil reportes al día.

Cabe precisar que OSIPTEL, recibe esta data de las empresas de telefonía, por lo que las estadísticas de denuncias (policiales y fiscales) difieren de este promedio.

1.3. Propuesta de la incorporación

La presente iniciativa legislativa busca proteger al usuario ante fraudes cibernéticos, hasta abril del 2022 se han registrado 7,297 denuncias ante el Ministerio Público, de las cuales 5,356 son delitos informáticos, 38,827 están relacionados al fraude informático, 946 a la suplantación

[12] INDECOPI. Informe Anual sobre el Estado de la Protección de los Consumidores en el Perú – 2020. https://bit.ly/3LKYiPE

[13] OSIPTEL. Comunicado Información de Osiptel sobre Equipos Móviles Robados Corresponde a Reportes Diarios de Usuarios a las Empresas Operadoras. https://bit.ly/3SJWUz3

de identidad y 110 a la estafa agravada para acceder o sustraer datos de tarjetas de ahorro o crédito[14].

A pesar de las cifras alarmantes, las empresas del sistema financiero no estarían implementado los mecanismos tecnológicos, que pueda arremeter contra la ciberdelincuencia, como hemos visto, se reportan casos de disposición de dinero en efectivo, compras virtuales, solicitud de préstamos, etc. y, en la actualidad, la carga recae sobre el consumidor, es él quien debe de presentar los medios de prueba correspondientes que demuestre haber sufrido este fraude, en muchos casos las empresas no llegan a reconocer las operaciones fraudulentas o demoran en exceso resolver, hecho que causa en los usuarios no solo daño económico sino también un daño emocional.

Según el Reglamento para la gestión de seguridad de la información y ciberseguridad[15], emitido por la SBS, las empresas del sistema financiero se encuentran en la obligación de implementar sistemas altamente tecnológicos para evitar estos delitos, en el mencionado reglamento se precisa lo siguiente:

> **Artículo 17. Implementación de los procesos autenticación**
> **17.1** La empresa debe implementar procesos de autenticación, conforme a la definición establecida en este Reglamento, para controlar el acceso a los servicios que provea a sus usuarios por canales digitales, previo a lo cual debe evaluar formalmente y tomar medidas sobre:
>
> a) El o los factores de autenticación que serán requeridos.
> b) Estándares criptográficos vigentes, basados en software o en hardware, y sus prestaciones de confidencialidad o integridad esperadas.
> c) Plazos y condiciones en las que será obligatorio requerir al usuario volver a autenticarse, lo que incluye y no se limita a casos por periodo de inactividad o sesiones de uso prolongado de sistemas.
> d) Línea base de controles de seguridad de la información requerida para prevenir las amenazas a que esté expuesto el proceso de autenticación, lo que incluye, y no se restringe, al número límite de intentos fallidos de autenticación, la prevención de ataques de interceptación y manipulación de mensajes.
> e) Lineamientos para la retención de registros de auditoría para la detección de amenazas conocidas y eventos de seguridad de la información.
>
> **17.2** Los procesos de autenticación deben ser reevaluados siempre que la tecnología utilizada para su implementación deje de contar con el soporte del fabricante, o tras el descubrimiento de nuevas vulnerabilidades que pueden exponerlos.
> **17.3** La empresa debe mantener y proteger los registros detallados de lo actuado en cada enrolamiento de usuario, intento de autenticación y cada operación que requiera de autenticación previa.
> **17.4** La empresa debe contar con herramientas y procedimientos para implementar el monitoreo de transacciones que permita tomar medidas

[14] El Peruano. Fraude Informático y Suplantación de Identidad son los Delitos Informáticos más denunciados. https://bit.ly/3foYjwr
[15] Superintendencia de Banca, Seguros y AFP. Resolución N° 504-2021

de reducción de la posibilidad de operaciones fraudulentas, que incorpore los escenarios de fraude ya conocidos, y el robo o compromiso de los elementos utilizados para la autenticación.

Siendo ello así, la Ley debe de establecer las medidas claras y necesarias con la finalidad de que las empresas del sistema financiero asuman la responsabilidad que deriva de la omisión de implementar los procesos de autenticación que arremetan contra la ciberdelincuencia, evitar el fraude cibernético y proteger al consumidor frente a una situación de esta naturaleza de tal manera que sus ahorros no se vean afectados, ni tampoco se vea afectada su reputación financiera ante la solicitud de préstamos por parte de los ciberdelincuentes.

Por otro lado, mediante Resolución N° 6523-2013-SBS la SBS aprobó el Reglamento de Tarjetas de Crédito y débito, el mismo que en su sub capítulo I – Medidas de Seguridad Aplicables a las Tarjetas de Crédito y Débito, del capítulo IV establece las medidas de seguridad que deben adoptar las empresas del sistema financiero que emitan estos instrumentos.

Teniendo como referencia los reglamentos emitidos por el organismo encargado de la regulación y supervisión de las empresas del Sistema Financiero, es necesario, establecer en la Ley las responsabilidades que deberán asumir estas empresas ante el eventual incumplimiento de los dispuesto en los diferentes cuerpos normativos sobre la materia y que traiga consigo el perjuicio del usuario.

1.4. Experiencia Comparada

En el 2015 la Unión Europea (UE), a través de sus representantes en el Parlamento Europeo y el Consejo de la Unión Europea, aprobaron la directiva (UR) 2015/2366[16], mediante la cual, entre otros temas, busca fortalecer la protección al consumidor.

En sus considerandos (6) y (7), expresa los sustentos que motivan esta modificación y actualización de la normativa europea:

> Considerando lo siguiente:
> (...)
>
> (6) Resulta oportuno establecer nuevas disposiciones que colmen las lagunas legales y, a la vez, aporten más claridad jurídica y garanticen una aplicación uniforme del marco regulador en toda la Unión. Es preciso garantizar condiciones operativas equivalentes, tanto a los operadores ya existentes en el mercado como a los nuevos, y facilitar que los nuevos medios de pago lleguen a un mayor número de consumidores, **así como asegurar una elevada protección del consumidor en el uso de esos servicios de pago en toda la Unión**. Se prevé que ello generará eficiencia en todo el sistema de pago e incrementará la gama de servicios de pago disponibles y la transparencia de estos, reforzando al mismo tiempo la confianza de los consumidores en un mercado de pagos armonizado.

[16] DIRECTIVA (UE) 2015/2366 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 25 de noviembre de 2015

> (7) **En los últimos años, han aumentado los riesgos de seguridad de los pagos electrónicos**, debido a la mayor complejidad técnica de estos, el incesante incremento del volumen de pagos electrónicos en todo el mundo y los nuevos tipos de servicios de pago. **Disponer de servicios de pago fiables y seguros es condición esencial para el buen funcionamiento del mercado de servicios de pago**, por lo que **los usuarios de esos servicios deben gozar de la debida protección frente a tales riesgos.** Los servicios de pago son esenciales para el mantenimiento de actividades económicas y sociales de vital importancia.
> (El resaltado es nuestro)

La implementación de esta directiva trajo consigo objetivos específicos como colmar lagunas jurídicas existentes a consecuencia del avance de la tecnología que proporciona a los bancos la posibilidad de ofrecer a sus clientes una variedad de propuestas para el uso de medios remotos de pago, de tarjetas de crédito y débito, de páginas web para compras, entre otros, otro objetivo importante que se desprende de esta normativa es brindar seguridad al consumidor ante el uso de algún canal de pago virtual, los mismo que se van incrementando continuamente.

El diario español La Vanguardia en su artículo "¿Cuánto dinero te devolverá el banco si te roban o duplican la tarjeta?[17]" desarrolla y explica los alcances de dicha directiva, precisa qué dice sobre robo y uso fraudulento de las tarjetas, así como los casos de devolución y excepciones de dicho cuerpo normativo.

La experiencia de los Estados miembros de la UE, muestra la necesidad de actualizar nuestra legislación teniendo como fin mayor la protección al consumidor.

2. EFECTOS DE LA VIGENCIA DE NORMA EN LA LEGISLACIÓN NACIONAL

La presente norma no colisiona con ningún texto constitucional, sino por el contrario, lleva concordancia con el artículo 65 de la Constitución Política del Perú el mismo que a la letra prescribe lo siguiente:

> Artículo 65.- **El Estado defiende el interés de los consumidores y usuarios**. Para tal efecto garantiza el derecho a la información sobre los bienes y servicios que se encuentran a su disposición en el mercado. Asimismo vela, en particular, por la salud y la seguridad de la población. (el resaltado es nuestro)

Asimismo, fortalecerá al Código de Protección y Defensa del Consumidor, representando el presente texto normativo el inicio del reconocimiento oportuno ante operaciones no reconocidas por parte de los usuarios del sistema financiero. En la actualidad, la Ley 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros no estipula en ninguno de sus artículos los temas y responsabilidades relacionadas al fraude informático, por lo que su modificación es necesaria tomando en consideración los índices de incidencia de este tipo de delitos.

---

[17] La Vanguardia. ¿Cuánto dinero te devolverá el banco si te roban o duplican la tarjeta?. https://bit.ly/3ClMyQq

3. VINCULACIÓN CON EL ACUERDO NACIONAL

La presente iniciativa se ha desarrollado en concordancia con las siguientes Políticas de Estado:

> ***"Tercera, Competitividad del País***
> *17. Afirmación de la economía social de mercado*
>
> *Nos comprometemos a **sostener la política económica del país sobre los principios de la economía social de mercado**, que es de libre mercado, pero conlleva el **papel insustituible de un Estado** responsable, promotor, **regulador**, transparente y subsidiario, que busca lograr el desarrollo humano y solidario del país mediante un crecimiento económico sostenido con equidad social y empleo.*
> *Con este objetivo, el Estado: **(a) garantizará la estabilidad de las instituciones y las reglas de juego**; (b) promoverá la competitividad del país, el planeamiento estratégico concertado y las políticas de desarrollo sectorial en los niveles nacional, regional y local; (c) estimulará la inversión privada; (d) fomentará el desarrollo de la infraestructura; (e) **evitará el abuso de posiciones dominantes y prácticas restrictivas de la libre competencia y propiciará la participación de organizaciones de consumidores en todo el territorio**; (f) fomentará la igualdad de oportunidades que tiendan a la adecuada distribución del ingreso; y (g) propiciará el fortalecimiento del aparato productivo nacional a través de la inversión en las capacidades humanas y el capital fijo".*
>
> ***"24. Afirmación de un Estado eficiente y transparente***
> *Nos comprometemos a construir y mantener un Estado eficiente, eficaz, moderno y transparente al servicio de las personas y de sus derechos, y que promueva el desarrollo y buen funcionamiento del mercado y de los servicios públicos. Nos comprometemos también a que el Estado atienda las demandas de la población y asegure su participación en la gestión de políticas públicas y sociales, así como en la regulación de los servicios públicos en los tres niveles de gobierno. **Garantizaremos una adecuada representación y defensa de los usuarios de estos servicios, la protección a los consumidores y la autonomía de los organismos reguladores.***
> *Con este objetivo el Estado: (a) incrementará la cobertura, calidad y celeridad de la atención de trámites así como de la provisión y prestación de los servicios públicos, para lo que establecerá y evaluará periódicamente los estándares básicos de los servicios que el Estado garantiza a la población; (b) establecerá en la administración pública mecanismos de mejora continua en la asignación, ejecución, calidad y control del gasto fiscal; (c) dará acceso a la información sobre planes, programas, proyectos, presupuestos, operaciones financieras, adquisiciones y gastos públicos proyectados o ejecutados en cada región, departamento, provincia, distrito o instancia de gobierno; (d) pondrá en uso instrumentos de fiscalización ciudadana que garanticen la transparencia y la rendición de cuentas en todas las instancias de gobierno; (e) erradicará la utilización proselitista del Estado y la formación de clientelas; **(f) mejorará la capacidad de gestión del Estado mediante la reforma integral de la administración pública en todos sus niveles**; (g) reducirá los costos de acceso a los bienes y servicios públicos; y (h) revalorará y fortalecerá la carrera pública promoviendo el ingreso y la permanencia de los servidores que demuestren alta competencia y solvencia moral".*

4. VINCULACIÓN CON LA AGENDA LEGISLATIVA

Mediante Resolución legislativa N° 002-2021-2022 del Congreso de la República aprobó la Agenda Legislativa, siendo ello así, la presente iniciativa

legislativa está relacionada con los temas 43 y 44 de la Política de Estado 17, del objetivo III:

III. COMPETITIVIDAD DEL PAÍS	17.AFIRMACIÓN DE LA ECONOMÍA SOCIAL DE MERCADO	42. Mejora de los organismos reguladores
		43. Apoyo a las asociaciones de defensa de los consumidores y usuarios
		44. Medidas a favor de los consumidores
		45. Promoción de la libre competencia
	18.BÚSQUEDA DE LA COMPETITIVIDAD, PRODUCTIVIDAD Y FORMALIZACIÓN DE LA ACTIVIDAD ECONÓMICA	46. Leyes de apoyo a las micro y pequeñas empresas
		47. Leyes de apoyo a los emprendedores
		48. Leyes para promover la formalización de la actividad empresarial
		49. Leyes de promoción del turismo
		50. Promoción de la inversión en el sector energía y minas
		51. Leyes de apoyo a la actividad empresarial

5. ANÁLISIS COSTO BENEFICIO

La aplicación de la presente medida no genera gastos adicionales en el Presupuesto del Sector Púbico, toda vez que el beneficio será fortalecer la legislación en la materia y contribuir a la protección de los derechos de los consumidores, sin demandar recursos adicionales al Tesoro Público. Cabe precisar que, según el INEI[18] el 53,2% de la población de 18 a más años de edad accedió al sistema financiero, por lo tanto, el beneficio de la presente iniciativa legislativa alcanzará a un número importante de usuarios del Sistema Financiero.

[18] INEI. Nota de Prensa - El 53,2% de la población de 18 y más años de edad accedió al sistema financiero. 20/06/2022.