



G.P. PODEMOS PERÚ

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"



Sumilla: Ley de protección a los usuarios de servicios financieros para la prevención y sanción de fraudes informáticos

El Congresista de la República **ENRIQUE WONG PUJADA**, integrante del **Grupo Parlamentario Podemos Perú**, en ejercicio de las facultades que le confiere el artículo 107 de la Constitución Política del Perú, y de conformidad con lo establecido en los artículos 75 y 76 del Reglamento del Congreso, presenta la siguiente iniciativa legislativa;

El Congreso de la República;

Ha dado la Ley siguiente:

LEY DE PROTECCIÓN DE LOS USUARIOS FINANCIEROS PARA PREVENIR Y SANCIONAR LOS FRAUDES INFORMÁTICOS

Artículo 1.- Objeto de la Ley

La presente ley tiene por objeto establecer medidas de protección a los usuarios de servicios financieros para la prevención y sanción de los fraudes informáticos, a través de la consolidación de denuncias ciudadanas, las que se realizan por medio de ventanillas virtuales, contribuyendo con la Policía Nacional del Perú en la recopilación de información.

Artículo 2.- Ventanilla virtual para la prevención de los fraudes informáticos

Dispóngase la creación de la "Ventanilla virtual para la prevención de los fraudes informáticos," en la que los usuarios de los servicios financieros y ciudadanos en general, denuncien los números telefónicos y correos electrónicos desde los cuales se emitan mensajes y enlaces web, para la comisión de fraudes informáticos.

Artículo 3.- Ente rector de la "Ventanilla virtual para la prevención de los fraudes informáticos"

La Policía Nacional del Perú, a través de su dirección competente, es el órgano rector de la "Ventanilla virtual para la prevención de los fraudes informáticos," encargada de la administración, recepción, consolidación, investigación y otros de los números telefónicos y

correos electrónicos denunciados por los usuarios de los servicios financieros y ciudadanos en general.

Artículo 4.- Procedimientos

4.1.- En la "Ventanilla virtual para la prevención de los fraudes informáticos", con la finalidad que la Policía Nacional del Perú consolide y realice la investigación respectiva se procede a:

4.1.1 Reportar el número telefónico o correo electrónico desde el cual se hacen llegar mensajes destinados a la comisión de fraudes informáticos.

4.1.2 Adjuntar la captura de pantalla, así como los enlaces a los que se pretenda redirigir al consumidor de los servicios financieros.

4.2.- La Policía Nacional del Perú en el marco de lo previsto en la Tercera y Cuarta Disposición Complementaria Final de la Ley 30096, Ley de Delitos Informáticos, realiza las investigaciones con las entidades del sector público, así como con los operadores privados.

4.3. La Policía Nacional del Perú comunica a los operadores de telecomunicaciones y al Organismo Supervisor de Inversión Privada en Telecomunicaciones para que procedan a bloquear las líneas telefónicas, direcciones electrónicas y enlaces web, lo que debe hacerse de manera inmediata.

Artículo 5.- Entidades obligadas a difundir la "Ventanilla virtual para la prevención de los fraudes informáticos"

Están obligadas a tener en sus páginas web la "Ventanilla virtual para la prevención de los fraudes informáticos", las siguientes entidades:

5.1.- Los ministerios.

5.2.- La Superintendencia de Banca, Seguros y AFP.

5.3.- El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.

5.4.- El Organismo Supervisor de Inversión Privada en Telecomunicaciones.

5.5.- La Policía Nacional del Perú.

5.6.- Las entidades del sistema financiero, supervisadas por la Superintendencia de Banca, Seguros y AFP.

Artículo 6.- Campañas de Difusión

Las entidades previstas en el artículo 5 de la presente norma, realizan campañas de difusión y educación sobre la "Ventanilla virtual para la prevención de los fraudes informáticos".

DISPOSICIONES COMPLEMENTARIAS

Primera: Aplicación del Decreto Legislativo 1182

Para la consecución de los objetivos de la presente norma se aplica las disposiciones previstas en el Decreto Legislativo 1182, Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado.

Segunda: Reglamentación

EL Poder Ejecutivo dentro de los sesenta (60) días de publicada la presente norma expide el reglamento.

Lima, setiembre del 2021



Firmado digitalmente por:
WONG PUJADA Enrique FIR
10821836 hard
Motivo: Soy el autor del
documento
Fecha: 05/10/2021 10:18:50-0500

ENRIQUE WONG PUJADA
Congresista de la República



Firmado digitalmente por:
CALLE LOBATON Digna FAU
20181749126 soft
Motivo: Soy el autor del
documento
Fecha: 05/10/2021 15:07:23-0500



Firmado digitalmente por:
LUNA GALVEZ Jose Leon FAU
20181749126 soft
Motivo: Soy el autor del
documento
Fecha: 05/10/2021 14:53:09-0500



Firmado digitalmente por:
LUNA GALVEZ Jose Leon FAU
20181749126 soft
Motivo: Soy el autor del
documento
Fecha: 05/10/2021 14:53:31-0500



CONGRESO DE LA REPÚBLICA

Lima, **18** de **octubre** del **2021**

Según la consulta realizada, de conformidad con el Artículo 77° del Reglamento del Congreso de la República: pase la Proposición **N° 398** para su estudio y dictamen, a la (s) Comisión (es) de:

- 1. DEFENSA DEL CONSUMIDOR Y ORGANISMOS REGULADORES DE LOS SERVICIOS PÚBLICOS**

HUGO ROVIRA ZAGAL
Oficial Mayor
CONGRESO DE LA REPÚBLICA

EXPOSICIÓN DE MOTIVOS

1) Antecedentes Legislativos

Como antecedentes legislativos podemos considerar a las siguientes normas:

- Ley 30096, Ley de Delitos Informáticos, que establece dentro del capítulo de delitos informáticos contra el patrimonio, al "Fraude Informático".
- Decreto Legislativo 1182, Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado y su modificatoria la Ley 31284.

No se ha encontrado antecedentes de iniciativas legislativas referidas al extremo de la propuesta.

2) Problema que se pretende resolver

El problema que se aborda y pretende combatir, es el denominado "phishing", entendido como el "método para engañar y hacer que se comparta contraseñas, números de tarjeta de crédito, y otra información confidencial haciéndose pasar por una institución de confianza en un mensaje de correo electrónico o llamada telefónica."¹, otorgando a la Policía Nacional del Perú la información proveniente de varios usuarios a fin de que esta pueda consolidarla y tener mayores elementos para su investigación, en especial bajo la modalidad de "smishing", cuya característica es que se realiza mediante mensajes de texto (SMS) conteniendo un enlace, con la finalidad de sustraer dinero de sus cuentas bancarias.

3) Fundamentos

La ciberdelincuencia no tiene límites ni fronteras, y es un proceso dinámico que se realiza en el anonimato, aprovechando el continuo desarrollo tecnológico, y a su vez el desconocimiento de las personas.

¹<https://www.google.com/search?q=phising&oq=phising&aqs=chrome..69i57j0i10i433j0i10i131i433j0i10i17.2328j0j15&sourceid=chrome&ie=UTF-8>

De acuerdo al informe "Ciberdelincuencia en el Perú: pautas para una investigación fiscal especializada"², la ocurrencia de estos delitos ha aumentado exponencialmente "de octubre de 2013 a julio de 2020, las fiscalías penales y mixtas registraron 21,687 denuncias, de las cuales el 40% proviene del 2019. Sin embargo, en ese mismo periodo se archivó el 58% de las mismas y se emitieron tan solo 108 sentencias, generando una importante carga fiscal y una sensación de impunidad e inseguridad".

Como se aprecia el nivel de resolución de casos con una sentencia condenatoria es sumamente bajo, 108 sentencias de 21, 687 denuncias, y esto se debe principalmente a la dificultad propia de la investigación por los métodos con los cuales se cometen los crímenes, así como por la falta de información con los que cuenta las unidades especializadas de la Policía Nacional del Perú.

Tabla 1. Denuncias de delitos informáticos investigados por la DIVINDAT. 2013-2020

DELITO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
Abuso de mecanismos y dispositivos informáticos	14	3	6	4	5	1	2	19	54	0.4%
Abuso de mecanismos y dispositivos informáticos	14	3	6	4	5	1	2	19	54	
Suplantación de identidad	10	101	114	134	132	227	247	572	1537	12.6%
Suplantación de identidad	10	101	114	134	132	227	247	568	1533	
Suplantación de identidad virtual								4	4	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	9	9			29	94	49	100	290	2.4%
Contra la indemnidad sexual de menores								2	2	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	9	9			29	94	49	98	288	
Contra datos y sistemas informáticos	38	62	47	47	104	126	159	177	760	6.2%
Acceso ilícito	11	42	1	1	49	84	129	151	468	
Acceso ilícito a una base de datos								2	2	
Atentado a integridad de datos informáticos	21	4	30	22	40	26	5	9	157	
Atentado a la integridad de sistemas informáticos	6	16	16	24	15	9	5	9	100	
Atentado contra la integridad de datos y sistemas informáticos						7	20	6	33	
Contra la intimidad y el secreto de las comunicaciones						3	2	8	13	0.1%
Intercepción de datos								2	2	
Intercepción de datos personales								1	1	
Tráfico ilegal de datos						3	2	5	10	
Fraude informático	298	334	414	610	1219	1928	2097	2615	9515	78.2%
Clonación de tarjeta	83	42	46	44	30	120	25	4	394	4
Compras fraudulentas por internet						287	431	261	979	10
Operaciones y transferencia electrónicas y/o de fondos no autorizados	215	292	368	566	1189	1521	1641	2350	8142	86
TOTAL	369	509	581	795	1489	2379	2556	3491	12169	100.0%

Adaptado de informe N° 237-2020-DIRINCRI-PNP/DIVINDAT-SEC, de fecha 14 de septiembre de 2020 y de información remitida por el Coronel Orlando Mendieta, jefe de DIVINDAT, a la OFAEC de fecha 20 de enero de 2021.

² Fiscalía de la Nación: Oficina de Análisis Estratégico Contra la Criminalidad / febrero 2021

De acuerdo a la información proporcionada por la Fiscalía de la Nación³ y como se muestra en el cuadro anterior, el 78.2% de las denuncias investigadas por la Divindat,⁴ corresponden a fraude informático, seguido de un 12.6% por delitos de suplantación de identidad.

Nos encontramos entonces que la mayoría de los de los delitos informáticos, están referidos a fraude informático.

La diferencia sustancial entre "Fraude Convencional" y "Fraude Informático", es que este último busca un beneficio económico.

Con relación al fraude informático, podemos señalar que éste se produce en su mayoría de los casos de forma masiva, pero en escalas -relativamente- pequeñas, es decir, los ciberdelincuentes no atacan un banco o una gran institución para apoderarse ilegalmente de millones de soles o dólares, sino lo que hacen, es tener como objetivo en cada ataque, a cientos o miles de ciudadanos, para sustraerles, "pequeñas cantidades" de dinero de sus cuentas bancarias.

Como lo hemos señalado, si bien los casos que son investigados por la Divindat y que siguen su curso en el Ministerio Público, son miles, y van en aumento en el último año, estos responderían únicamente a una parte de los crímenes, siendo las tentativas una suma muy superior, que podría llegar a millones de intentos cada año, las cuales no son denunciadas y/o tramitadas ante el Ministerio Público.

En efecto, Lima concentra el mayor número de denuncias que siguen su curso ante alguna dependencia del Ministerio Público⁵ con un 61%, seguido de Arequipa con un 6%, La Libertad con 5% y Lambayeque con 4%.

³ Informe "Ciberdelincuencia en el Perú: pautas para una investigación fiscal especializada"

⁴ División de Investigación de Delitos de Alta Tecnología

⁵ Informe "Ciberdelincuencia en el Perú: pautas para una investigación fiscal especializada"

Tabla 3. Denuncias por delitos informáticos registradas en Fiscalías Penales Comunes y Fiscalías Mixtas, de octubre 2013 a julio 2020

DELITO SUBGENÉRICO	2013	2014	2015	2016	2017	2018	2019	2020	TOTAL	%
LIMA	67	325	550	708	1495	2366	3713	1116	10 340	47.68%
LIMA NORTE	3	24	24	99	174	357	717	220	1618	7.46%
AREQUIPA	1	18	47	155	255	291	506	115	1388	6.40%
LIMA ESTE	3	17	26	53	147	251	603	183	1283	5.92%
LA LIBERTAD	3	20	35	36	94	213	487	232	1120	5.16%
LAMBAYEQUE	1	11	31	82	119	182	326	124	876	4.04%

Los principales medios de comunicación⁶, han dado cuenta esta semana que Perú registró más de 4.700 millones de intentos de ciberataques en 2021⁷ durante el primer semestre.

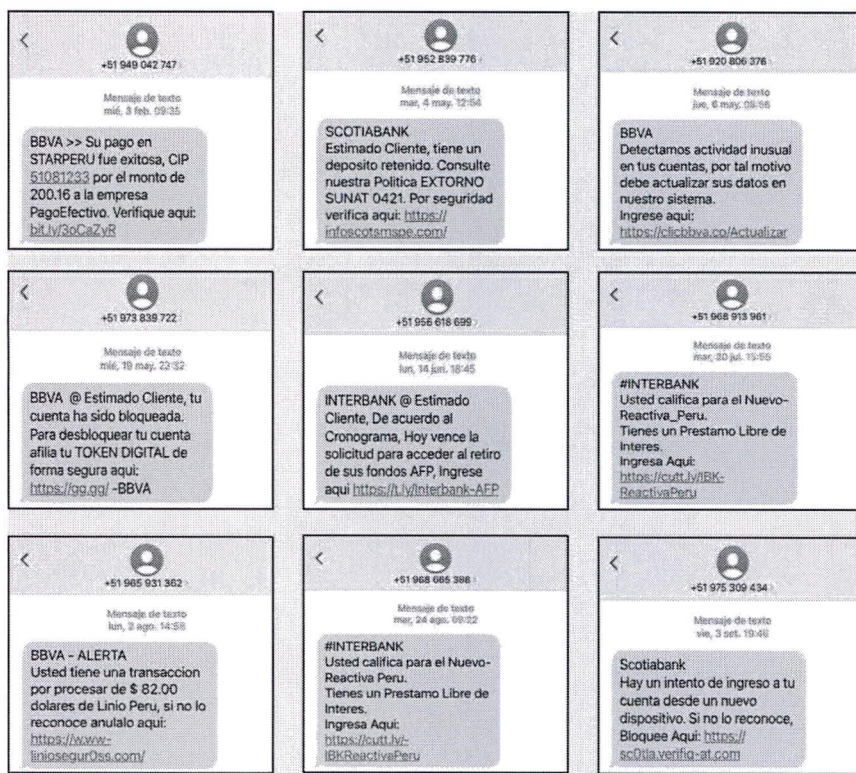
Como hemos expuesto, la principal modalidad de los fraudes informáticos se hace mediante "smishing", cuya característica es que se realiza mediante mensajes de texto (SMS) conteniendo un enlace, con la finalidad de sustraer dinero de sus cuentas bancarias.

Esta ilegal práctica se realiza de manera masiva, en simultaneo a cientos o miles de usuarios, y está destinada a que una parte de ellos, "caiga en la trampa", siendo que solo los que son realmente afectados proceden a denunciar el hecho –al menos ante su banco- y una cantidad menor ante la policía y el Ministerio Público.

A continuación, mostramos los "smishing", que han sido enviados a una sola persona en el periodo de 7 meses, las cuales no son denunciadas a la policía nacional y ni siquiera reportadas al operador de telecomunicaciones.

⁶ El Comercio, La República, RPPP

⁷ <https://larepublica.pe/tecnologia/2021/09/23/peru-sufrio-mas-de-4700-millones-de-intentos-de-ciberataques-en-2021/>



Todos ellos, son enviados por mensaje de texto, conteniendo un mensaje destinado a engañar al destinatario y por último un enlace, al que, de ingresar, se proporcionaría información personal de contraseñas a los ciberdelincuentes, procediendo estos a sustraer el dinero.

Esta modalidad de estafa se realiza de manera masiva, con bases de datos conseguida en muchos casos de manera ilegal, esperando que al menos una parte o una fracción de los destinatarios acceda al enlace y sustraigan sumas de dinero de sus cuentas bancarias.

EFFECTO DE LA VIGENCIA DE LA NORMA EN LA LEGISLACIÓN NACIONAL

La presente propuesta, busca establecer un marco normativo para otorgarle elementos suficientes a la Policía Nacional del Perú para la investigación y denuncias de los fraudes informáticos, ello a través denuncias ciudadanas, las que se realizan a través de ventanillas virtuales, colocadas en la página web de los ministerios, de la Policía Nacional del Perú, la Superintendencia de Banca, Seguros y AFP, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, el Organismo Supervisor de Inversión Privada en Telecomunicaciones y

de las entidades del sistema financiero, supervisadas por la Superintendencia de Banca, Seguros y AFP

Asimismo, se busca que ante tales reportes se proceda a bloquear, número telefónicos, correos y enlaces web – de manera inmediata- para evitar que haya un mayor número de víctimas.

La Policía Nacional del Perú con la información proporcionada por los usuarios de los servicios financieros y ciudadanía en general, procede conforme a las atribuciones que le otorga el Decreto Legislativo 1182, Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado y su modificatoria la Ley 31284.

ANÁLISIS COSTO BENEFICIO

La presente norma no genera costo alguno al erario nacional, por cuanto busca la creación de una ventanilla virtual, en las páginas web existentes de los diversos ministerios, así como de la Policía Nacional del Perú, reguladores y supervisores y de las entidades financieras privadas, donde los usuarios de los servicios financieros y ciudadanos en general puedan denunciar los intentos de fraudes informáticos.

Con la información consolidada por la Policía Nacional del Perú -a través de su área correspondiente- se destinarán los recursos humanos y materiales, con mayor eficiencia para la investigación y denuncia de los fraudes informáticos.

En cuanto a los efectos monetarios y su impacto económico, éste se vería reflejado en las personas a las que se evitó que sean víctimas de fraude informático.

La presente propuesta no tiene impacto ambiental por regular un mecanismo de denuncia ciudadana a través de ventanillas virtuales a fin de dotar a la Policía Nacional del Perú de información para que ella proceda con la investigación y denuncia de los fraudes informáticos conforme a sus facultades.

VINCULACIÓN CON LAS POLÍTICAS DEL ACUERDO NACIONAL

Sétima Política: Erradicación de la violencia y fortalecimiento del civismo y de la seguridad ciudadana

Por el cual se da el compromiso a normar y fomentar las acciones destinadas a fortalecer el orden público y el respeto al libre ejercicio de los derechos y al cumplimiento de los deberes individuales, señalándose que... "(f) desarrollará una política de especialización en los organismos públicos responsables de garantizar la seguridad ciudadana".

Vigésima Cuarta: Afirmación de un Estado eficiente y transparente

Por el cual se da el compromiso de 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, señalándose que... "(f) mejorará la capacidad de gestión del Estado mediante la reforma integral de la administración pública en todos sus niveles".