Proyecto de Ley N° 9443/2024-CR

ESDRAS RICARDO MEDINA MINAYA

CONGRESO
REPÚBLICA

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
" Año del Bicentenario, de la Consolidación de nuestra independencia, y de la Conmemoración de las heroicas batallas de Junín y Ayacucho

CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO
06 NOV. 2024
RECIBIDO
Firma: Hora: 8:43

PROYECTO DE LEY QUE PROTEGE A LOS PERUANOS FRENTE A LAS AMENAZAS CIBERNÉTICAS

A iniciativa del **CONGRESISTA ESDRAS RICARDO MEDINA MINAYA,** miembro del Grupo Parlamentario **RENOVACIÓN POPULAR**, en ejercicio del derecho de iniciativa legislativa que les confiere el artículo 107° de la Constitución Política del Perú y de conformidad con los artículos 75° y 76° del Reglamento del Congreso de la República, proponen la siguiente iniciativa legislativa:

FÓRMULA LEGAL

PROYECTO DE LEY QUE PROTEGE A LOS PERUANOS FRENTE A LAS AMENAZAS CIBERNÉTICAS

Artículo 1. – Objeto de la Ley

La presente ley tiene como objetivo modificar los artículos 2 y 4 de la Ley de Delitos Informáticos Ley N° 30096 para adaptarla a los desafíos actuales en materia de ciberseguridad. Esta modificación busca fortalecer la protección de los ciudadanos peruanos frente a las amenazas del cibercrimen, garantizando un marco legal actualizado.

Artículo 2. – Finalidad de la Ley

La presente ley tiene como finalidad actualizar la normativa vigente para alinearla con las exigencias del Convenio de Budapest, del cual Perú es parte. Este tratado internacional establece estándares que fomentan la cooperación y la armonización de las legislaciones en la lucha contra los delitos informáticos. Al adoptar estas normas, podremos mejorar nuestras capacidades de respuesta ante incidentes de ciberseguridad, fortaleciendo

así la protección de nuestros ciudadanos en el entorno digital.

Artículo 3. Modificación del artículo 2 y 4 de la Ley de Delitos Informáticos Ley N° 30096.

Modifíquese el artículo 2 y 4 de la Ley de Delitos Informáticos Ley N° 30096 bajo los siguientes términos:

Artículo 2. Acceso ilícito

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

Será reprimido con la misma pena, el que accede a un sistema informático con el ánimo de apoderarse, divulgar o utilizar la información contenida en el sistema informático.

Artículo 4. Atentado a la integridad de sistemas informáticos:

El que deliberada e ilegítimamente **obstaculice o impida el normal funcionamiento, total o parcialmente, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos**, será reprimido con pena privativa

de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."

DISPOSICIÓN COMPLEMENTARIA

UNICA. – Reglamentación

El Poder Ejecutivo, en plazo de máximo de sesenta (60) días calendarios, aprueba las normas reglamentarias que correspondan, conforme a lo dispuesto en la presente ley.

Lima, 05 de octubre de 2024.

FIRMA DIGITAL
Firmado digitalmente por: MUÑANTE BARRIOS Alejandro FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 06/11/2024 12:26:57-0500

Firmado digitalmente por: MUÑANTE BARRIOS Alejandro FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 06/11/2024 12:27:13-0500

FIRMA DIGITAL
Firmado digitalmente por: JAUREGUI MARTINEZ DE AGUAYO Maria De Los Milagros Jackeline FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 06/11/2024 13:36:47-0500

FIRMA DIGITAL
Firmado digitalmente por: TRIGOZO REÁTEGUI Cheryl FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 06/11/2024 16:37:58-0500

FIRMA DIGITAL
Firmado digitalmente por: CICCIA VASQUEZ Miguel Angel FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 06/11/2024 17:29:59-0500

FIRMA DIGITAL
Firmado digitalmente por: ZEBALLOS APONTE Jorge Arturo FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 06/11/2024 18:23:30-0500

FIRMA DIGITAL
Firmado digitalmente por: MEDINA MINAYA Esdras Ricardo FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 06/11/2024 18:53:37-0500

FIRMA DIGITAL
Firmado digitalmente por: CORDOVA LOBATON Maria Jessica FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 06/11/2024 20:09:40-0500

CONGRESO DE LA REPÚBLICA

Lima, **08** de **noviembre** de **2024**

Según la consulta realizada, de conformidad con el Artículo 77° del Reglamento del Congreso de la República: pase la Proposición **N° 9443/2024-CR** para su estudio y dictamen, a la (s) Comisión (es) de:

1. **JUSTICIA Y DERECHOS HUMANOS.**

GIOVANNI FORNO FLOREZ
Oficial Mayor
CONGRESO DE LA REPÚBLICA

EXPOSICIÓN DE MOTIVOS

La presente ley tiene como objetivo modificar los artículos 2 y 4 de la Ley de Delitos Informáticos (Ley N° 30096) para adaptarla a los desafíos actuales en materia de ciberseguridad. Esta modificación busca fortalecer la protección de los ciudadanos peruanos frente a las crecientes amenazas del cibercrimen, garantizando así un marco legal que esté a la altura de la evolución tecnológica y de los riesgos emergentes.

En un contexto de globalización y rápida evolución de las tecnologías, han surgido nuevas formas de ciberdelincuencia que afectan a gobiernos, empresas y ciudadanos a nivel mundial. La ciberdelincuencia se define como la comisión de delitos mediante sistemas informáticos o medios de comunicación masivos, tales como teléfonos, computadoras y dispositivos móviles.

Desde la promulgación de la Ley de Delitos Informáticos el 22 de octubre de 2013, se han implementado mecanismos para prevenir y sancionar delitos que vulneran sistemas y datos informáticos, así como otros bienes jurídicos esenciales.

Sin embargo, la rápida evolución de las tecnologías y el aumento de la complejidad de los delitos informáticos exigen una revisión y actualización de dicho marco normativo.

CONVENIO DE BUDAPEST

El 'Convenio sobre la Ciberdelincuencia' o 'Convenio de Budapest' es un instrumento jurídico que permite a los jueces y fiscales realizar requerimientos de cooperación internacional vinculados a delitos informáticos, los que de

acuerdo a la legislación peruana se encuentran regulados en la Ley N.° 30096, modificada por la Ley N.°30171; informó la Unidad de Cooperación Judicial Internacional y de Extradiciones de la Fiscalía de la Nación.

Se trata de los delitos: de acceso ilícito; atentado contra la integridad de datos y sistemas informáticos; proposiciones a niñas, niños y adolescentes con fines sexuales por medios tecnológicos, tráfico ilegal e interceptación de datos informáticos, fraude, suplantación de identidad, y abusos de mecanismos y dispositivos.

Estos delitos también son objeto de conocimiento de la Ley N.° 30077, en virtud de su artículo N.° 3, cuando sean cometidos por una presunta organización criminal.

Cabe indicar que mediante el Decreto Supremo N.° 010-2019-RE del 10 de marzo del 2019, el gobierno peruano ratificó el Convenio sobre la Ciberdelincuencia y, a través de la publicación oficial en el Diario Oficial El Peruano, de fecha 22 de setiembre del 2019, se estableció su entrada en vigencia el 1 de diciembre de dicho año.

El Perú, al suscribir el Convenio, asumió el compromiso de la lucha frontal y efectiva contra la ciberdelincuencia y la necesidad de cooperación internacional rápida y eficaz en materia penal.[1]

INCREMENTO DE LA CIBERDELINCUENCIA EN LOS ÚLTIMOS AÑOS

La Defensoría del Pueblo en atribución a sus funciones realiza un imforme, titulado *"La ciberdelincuencia en el Perú: Estrategias y retos del Estado"* de

[1] https://www.gob.pe/institucion/mpfn/noticias/302628-convenio-sobre-la-ciberdelincuencia-permite-a-jueces-y-fiscales-realizar-requerimientos-de-cooperacion-internacional

mayo de 2023, **las denuncias por ciberdelincuencia se han cuadruplicado entre el 2018 y 2021**, según los datos siguientes:

- Año 2018 – 3,031 denuncias
- Año 2019 – 7,814 denuncias
- Año 2020 – 9,787 denuncias
- Año 2021 – 12,827 denuncias

Dado que muchos delitos informáticos trascienden fronteras, una ley actualizada facilitará la colaboración con otras naciones y organismos internacionales, permitiendo una respuesta más coordinada ante el cibercrimen global.

Este alarmante incremento subraya la necesidad urgente de modificar la legislación existente para enfrentar eficazmente los desafíos del ciberespacio

LOS CIBERDELITOS CON MÁS DENUNCIAS

De acuerdo con dicho informe, los tipos de ciberdelitos frecuentemente denunciados ante la Policía son:

1. fraude informático
2. suplantación de identidad
3. abuso de mecanismos
4. dispositivos informáticos
5. atentado a la integridad de datos informáticos
6. grooming online
7. acceso ilícito

CONTEXTO DEL CASO INTERBANK

En octubre de 2023, Interbank sufrió una vulneración a su sistema de seguridad, enfrentó una filtración de datos que afectó a un grupo de clientes. La entidad bancaria comunicó que la exposición de datos fue resultado de la acción de un tercero no autorizado, lo que generó inquietud entre sus usuarios respecto a la seguridad de su información personal y financiera. A pesar de la preocupación inicial, Interbank aseguró que los depósitos y productos financieros de sus clientes estaban protegidos.

Importancia de la Lucha Contra los Delitos Informáticos

1. Proteger la Información del Consumidor: La filtración de datos de Interbank pone de manifiesto la vulnerabilidad de la información personal en el entorno digital. La modificación de la Ley de Delitos Informáticos busca establecer un marco legal que fortalezca la protección de los datos de los ciudadanos.

2. Adaptación a Nuevos Desafíos: La ciberseguridad es un campo en constante evolución. Las leyes existentes deben ser revisadas y adaptadas para abordar nuevas amenazas y métodos de ataque. La modificación de los artículos 2 y 4 de la ley busca proporcionar herramientas legales más efectivas para combatir el cibercrimen, permitiendo una respuesta más ágil ante incidentes como el de Interbank.

3. Responsabilidad de las Instituciones: La filtración de datos enfatiza la responsabilidad de las instituciones financieras en la gestión de la seguridad de la información.

El caso de Interbank es un claro ejemplo de los riesgos asociados con el uso de tecnologías digitales en el sector financiero. La modificación de la Ley de Delitos Informáticos es un paso necesario para fortalecer la ciberseguridad y proteger a los ciudadanos peruanos de los delitos informáticos.

A fin de salvaguardar los intereses de todos los peruanos se presenta la propuesta de modificación en el siguiente cuadro comparativo:

LEY N° 30096 (vigente)	PROPUESTA DE MODIFICACIÓN
Artículo 2. Acceso ilícito El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."	Artículo 2. Acceso ilícito El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa." **Será reprimido con la misma pena, el que accede a un sistema informático**

LEY N° 30096 (vigente)	PROPUESTA DE MODIFICACIÓN
(...)	**con el ánimo de apoderarse, divulgar o utilizar la información contenida en el sistema informático.**
"Artículo 4. Atentado a la integridad de sistemas informáticos	Artículo 4. Atentado a la integridad de sistemas informáticos:
El que deliberada e ilegítimamente ~~inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios,~~ será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."	El que deliberada e ilegítimamente **obstaculice o impida el normal funcionamiento, total o parcialmente, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos**, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."

EFECTOS DE LA VIGENCIA DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

El presente Proyecto de Ley se enmarca dentro de la Constitución, ya que no contradice ningún artículo de nuestra Carta Magna. Su objetivo principal es proteger a la ciudadanía peruana en un mundo cada vez más digitalizado. En este contexto, es crucial que tanto las instituciones como el marco legal evolucionen para hacer frente a los desafíos que plantea el cibercrimen. La implementación de esta ley no solo contribuirá a prevenir futuros incidentes,

sino que también fomentará la confianza del público en el uso de servicios financieros digitales

ANÁLISIS COSTO BENEFICIO

La presente iniciativa no implica gastos públicos ni requiere una ampliación del presupuesto de las universidades nacionales, ya que su propósito es abordar una problemática existente a nivel nacional. El caso como el de interbank puede deteriorar la confianza de los usuarios en las instituciones bancarias. Por lo tanto, un marco legal actualizado en materia de delitos informáticos es crucial; no solo protege a los usuarios, sino que también promueve la confianza en el uso de servicios digitales, los cuales son esenciales en la actualidad

I. VINCULACIÓN CON LAS POLÍTICAS DE ESTADO DEL ACUERDO NACIONAL

La presente iniciativa legislativa tiene relación con las siguientes Políticas de Estado establecidas en el Acuerdo Nacional.

I: Democracia y Estado de derecho, que contiene la política de Estado 7. referida a la " Erradicación de la violencia y fortalecimiento del civismo y de la seguridad ciudadana", en la que se proponen las siguientes líneas de acción: (a) consolidará políticas orientadas a prevenir, disuadir, sancionar y eliminar aquellas conductas y prácticas sociales que pongan en peligro la tranquilidad, integridad o libertad de las personas, así como la propiedad pública y privada;

De otro lado, en concordancia con séptima la Política de Estado, en la Agenda Legislativa 2023-2024 del Congreso de la República se han planteado los temas 18 y 20, referidos a MEDIDAS EN FAVOR DE LA SEGURIDAD

CIUDADANA Y EL CIVISMO y MODIFICACIONES AL CÓDIGO PENAL, respectivamente.