



GARCÍA CORREA IDELSO MANUEL

"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 Ayacucho"



LEY QUE ESTABLECE PENAS PRIVATIVAS DE LA LIBERTAD PARA EL DELITO DE EXTORSIÓN CIBERNÉTICA

El congresista que suscribe, **Idelso Manuel García Correa**, integrante del **Grupo Parlamentario Alianza para el Progreso**, en ejercicio de las facultades que le confiere el artículo 107° de la Constitución Política del Perú, y según lo estipulado en los artículos 75° y 76° del Reglamento del Congreso de la República, presenta a consideración del Congreso de la República el siguiente proyecto de Ley:

"LEY QUE ESTABLECE PENAS PRIVATIVAS DE LA LIBERTAD PARA EL DELITO DE EXTORSIÓN CIBERNÉTICA"

Artículo 1. Objeto de la Ley

La presente Ley tiene por objeto establecer penas privativas de la libertad para el delito de extorsión cibernética.

Artículo 2. Finalidad

La presente ley tiene por finalidad fortalecer la seguridad ciudadana en el país, al reducir la incidencia del delito de extorsión cibernética, el cual ya ha afectado a más de 15 mil personas en la actualidad.

Artículo 3. Modificación del artículo 200° del Código Penal

Modifíquese el artículo 200° del Código Penal, en los siguientes términos:

*"Artículo 200.- Extorsión
(....)*

La misma pena se aplicará al que, con la finalidad de contribuir a la comisión del delito de extorsión, suministra información que haya conocido por razón o con



GARCÍA CORREA IDELSO MANUEL

"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"

ocasión de sus funciones, cargo u oficio o proporciona deliberadamente los medios para la perpetración del delito.

El que, mediante uso de dispositivos electrónicos, sistemas informáticos y entornos digitales; obtiene acceso no autorizado de los dispositivos de una persona o los sistemas de una organización para sustraer información privada que le sirvan de sustento para valerse de amenazas y cualquier otro acto de intimidación con la finalidad de obtener una ventaja económica, la pena privativa de la libertad será no menor de diez ni mayor de quince años.

*El que, mediante violencia o amenaza, tomas locales, obstaculiza vías de comunicación o impide el libre tránsito de la ciudadanía o perturba el normal funcionamiento de los servicios públicos o la ejecución de obras legalmente autorizadas, con el objeto de obtener de las autoridades cualquier beneficio o ventaja económica indebida u otra ventaja de cualquier otra índole, será sancionado con pena privativa de libertad no menor de cinco ni mayor de diez años.
(....)"*

Artículo 4. incorporación del artículo 8-A en la Ley 30096, Ley de delitos informáticos

Incorpórese el artículo 8-A en la Ley 30096, Ley de delitos informáticos, en los siguientes términos:

"Artículo 8-A.- Extorsión cibernética (....)

El que mediante uso de dispositivos electrónicos, sistemas informáticos y entornos digitales; obtiene acceso no autorizado de los dispositivos de una persona o los sistemas de una organización para sustraer información privada que le sirvan de sustento para valerse de amenazas y cualquier otro acto de intimidación con la finalidad de obtener una ventaja económica, la pena privativa de la libertad será no menor de diez ni mayor de quince años."



GARCÍA CORREA IDELSO MANUEL

"Decreto 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"

DISPOSICIÓN COMPLEMENTARIA

ÚNICA. Reglamentación.

El Poder Ejecutivo aprueba el reglamento de la presente ley en un plazo no mayor de sesenta días calendarios, contados a partir de la publicación.



Firmado digitalmente por:
CHIABRA LEON Roberto
Enrique FAU 20181749128 soft
Motivo: Soy el autor del documento
Fecha: 18/11/2024 13:56:27-0500



Firmado digitalmente por:
JULON IRIGOIN Eva Edhit
FAU 20181749128 soft
Motivo: Soy el autor del documento
Fecha: 18/11/2024 15:12:09-0500



Firmado digitalmente por:
RUIZ RODRIGUEZ Magaly
Rosmary FAU 20181749128 soft
Motivo: Soy el autor del documento
Fecha: 18/11/2024 18:00:51-0500



Firmado digitalmente por:
HEIDINGER BALLESTEROS
Nelcy Lidia FAU 20181749128 soft
Motivo: Soy el autor del documento
Fecha: 18/11/2024 12:18:10-0500



Firmado digitalmente por:
SOTO REYES Alejandro FAU
20181749128 soft
Motivo: Soy el autor del documento
Fecha: 13/11/2024 14:24:49-0500



Firmado digitalmente por:
GARCIA CORREA Idelfo
Manuel FAU 20181749128 soft
Motivo: Soy el autor del documento
Fecha: 18/11/2024 09:52:47-0500



Firmado digitalmente por:
CAMONES SORIANO Lady
Mercedes FAU 20181749128 soft
Motivo: Soy el autor del documento
Fecha: 18/11/2024 13:01:07-0500

www.congreso.gob.pe

Plaza Bolívar, Av. Abancay s/n - Lima, Perú
Central Telefónica: 311-7777



Firmado digitalmente por:
SOTO REYES Alejandro FAU
20181749128 soft
Motivo: Soy el autor del documento
Fecha: 13/11/2024 14:24:34-0500



Firmado digitalmente por:
SALHUANA CAMDES Eduardo
FAU 20181749128 hard
Motivo: Soy el autor del documento
Fecha: 18/11/2024 11:49:14-0500



Firmado digitalmente por:
ACUÑA PERALTA Maria
Grimaneza FAU 20181749128 soft
Motivo: Soy el autor del documento
Fecha: 18/11/2024 11:50:40-0500



I. EXPOSICIÓN DE MOTIVOS

a) La extorsión cibernética en el país

Se entiende por extorsión cibernética al delito que consiste en el empleo de dispositivos electrónicos, sistemas informáticos, entornos digitales, redes y computadoras; para poder vulnerar los dispositivos de una persona o los sistemas de una organización para sustraer información privada que le sirvan de sustento para amenazar u obligar digitalmente a alguien a hacer algo en contra de su voluntad. Así, los cibercriminales amenazan con filtrar datos, lanzar ataques cibernéticos, deshabilitar operaciones, evitar que los usuarios accedan a los datos o destruir los datos robados si la víctima no paga algún tipo de rescate. La extorsión cibernética hace uso de numerosos métodos, como el doxxing, los ataques DDoS y el ransomware¹, los cuales se detallan a continuación:

1. Ataque DDoS: el ataque de denegación de servicio distribuido (DDoS) consiste en bloquear el tráfico normal de un servidor, mediante el uso de dispositivos de internet diseñados en sobrepasar y colapsar un servidor con tráfico de Internet, el cual termina por ralentizar o dejar fuera de funcionamiento al servidor. Los criminales cibernéticos amenazan a las organizaciones exigiendo pagos para detener el ataque DDoS o evitar que el ataque en sí se produzca.
2. Ransomware: en esta modalidad los cibercriminales usan un tipo de malware denominado ransomware que impide que los usuarios accedan a sus datos sensibles. Cuando se instala el ransomware en el dispositivo de un usuario, lo bloquea cifrando sus archivos o dispositivos. Los cibercriminales se pondrán en contacto con la víctima prometiendo devolverle el acceso después del pago de un rescate.

¹ Kaspersky. (2023). ¿Qué es la extorsión cibernética? <https://www.keepersecurity.com/blog/es/2024/01/15/what-is-cyber-extortion/#:~:text=La%20extorsi%C3%B3n%20cibern%C3%A9tica%20es%20una%20categor%C3%ADa%20generalizada%20de%20delito%20cibern%C3%A9tico,los%20cibercriminales%20lo%20que%20quieren.>



3. Doxxing: es un método por el cual un atacante cibernético publica en Internet información de identificación personal (PII) sobre su víctima como su dirección particular, los números de sus tarjetas de crédito o débito, o bien cualquier otra información confidencial. En el doxxing es necesario que los atacantes puedan recopilar la mayor cantidad de información posible sobre la víctima mediante ataques cibernéticos o información compartida públicamente (por ejemplo, las redes sociales), para luego una vez recopilada la información, amenacen con publicar información privada sobre las víctimas si estas no pagan una suma de dinero.

En el Perú, al igual que la mayoría de países de Latinoamérica, la ciberdelincuencia y particularmente la extorsión cibernética vienen ganando terreno en los últimos años; así se tiene que únicamente en Lima se han registrado en los años 2020 (4637 denuncias), 2021 (5404 denuncias), 2022 (4353 denuncias) y 1492 denuncias en el año 2023; dando un total de 15,616 personas que ya han sido víctimas de este tipo de delito².

Así mismo, recientemente se ha apreciado que la extorsión cibernética ha dejado de ser una amenaza para los ciudadanos de a pie, siendo que ahora entidades públicas y grandes empresas privadas ya han sido víctimas de este delito, lo que significa que ahora los cibercriminales se están especializando en realizar la extorsión cibernética a un nivel institucional y corporativo; como son los casos sufridos por la Municipalidad de Miraflores y el banco Interbank. En el caso de la Municipalidad de Miraflores, esta entidad sufrió un ciberataque que vulneró la información de más de 82 mil vecinos que habitan en este distrito a cambio de una suma de dinero, y en el segundo caso, se tiene la extorsión cibernética de la que el banco Interbank fue víctima en noviembre del presente año, cuando un grupo de hackers vulneraron su sistema de seguridad informático, comprometiendo la información de clientes de dicho banco; para luego los representantes de este banco pasar a ser contactados por los cibercriminales, los cuales

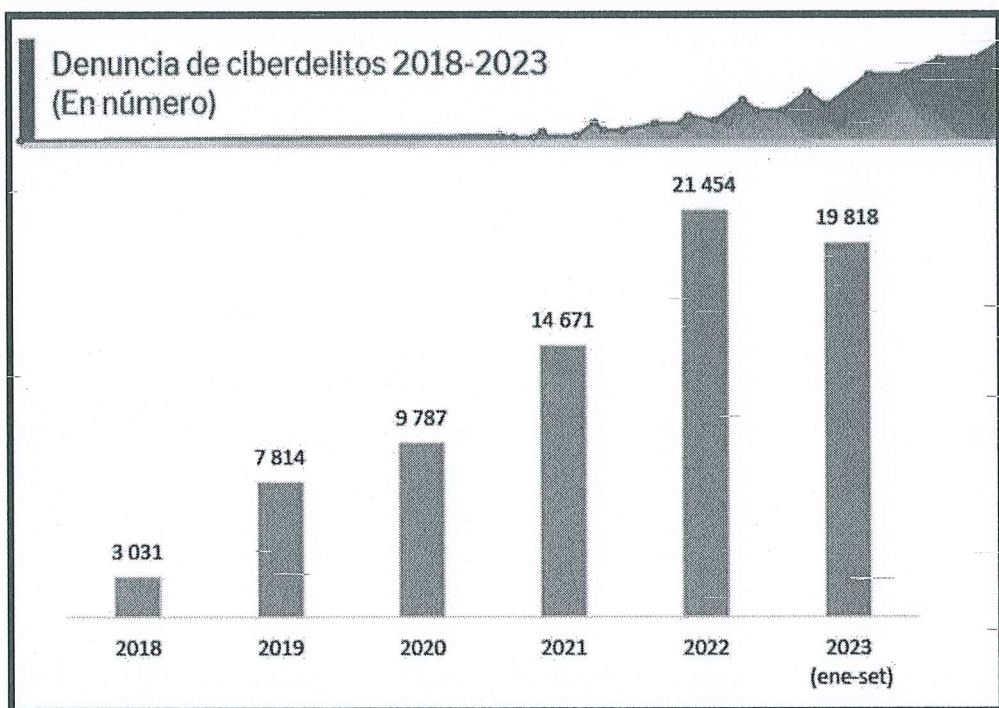
² IURA & ALex Abogados. (2024). La Ciberdelincuencia en el Perú. <https://il-abogados.pe>. <https://il-abogados.pe/blog/la-ciberdelincuencia-en-el-peru>



exigieron una fuerte suma de dinero (aproximadamente 04 millones de dólares), a cambio de devolver esta información al banco en mención³.

Se debe de tener en cuenta también, que si no contabilizamos únicamente la extorsión cibernética, sino a todos los ciberdelitos en general (y en donde se encuentran incluidos los casos de extorsión cibernética), se tiene que estos registran más de 50 mil casos en los últimos 03 años, con 19,818 casos en el 2023, 21,454 casos en el 2022 y 14,671 casos en el año 2021 de acuerdo lo informado por SIDPOL (Sistema Informático Desarrollado por la Policía Nacional del Perú) como se muestra en el siguiente cuadro:

INCIDENCIA DE CIBERDELITOS EN LOS ÚLTIMOS AÑOS EN EL PERÚ



Fuente: SIDPOL, disponible en el siguiente enlace web:
<https://lacamara.pe/inseguridad-ciudadana-en-el-peru-cifras-impactantes-y-soluciones-urgentes/>

³ Perú 21. (2024). El cibercrimen opera libre de sanciones. <https://peru21.pe>.
<https://peru21.pe/opinion/el-cibercrimen-opera-libre-de-sanciones-el-cibercrimen-opera-libre-de-sanciones-por-alvina-ruiz>

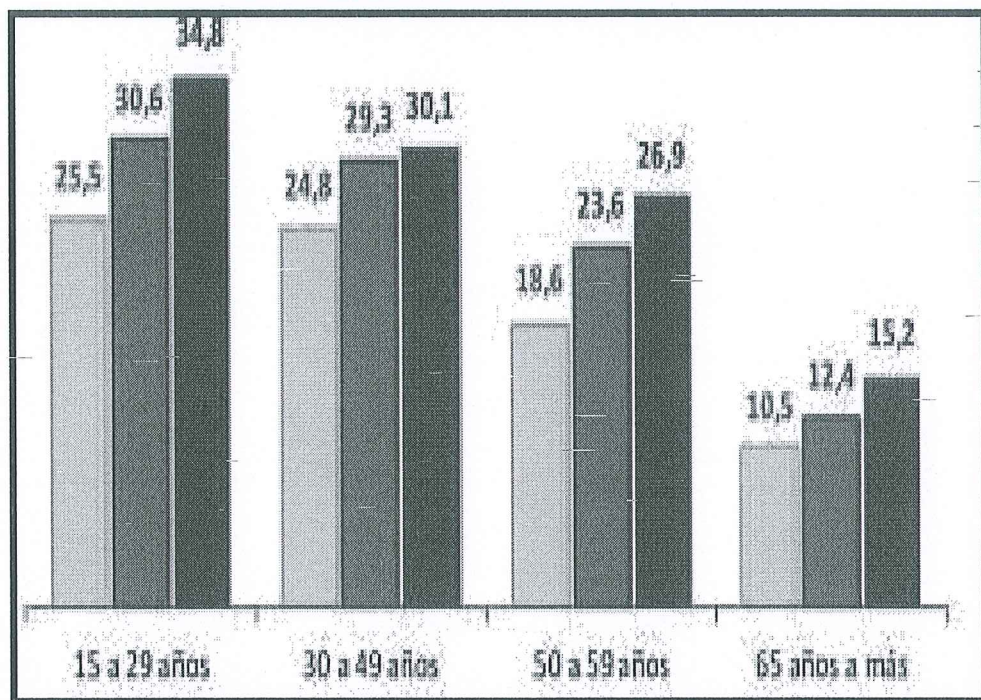


GARCÍA CORREA IDELSO MANUEL

"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"

Estas cifras confirmarían lo señalado por la Policía Nacional de Perú, en el que nuestro país es uno de los países más afectados por la cibercriminalidad a nivel mundial. Además, con respecto a los grupos de edad de la población afectada por algún ciberdelito, es en el grupo de las personas entre los 15 y 29 años de edad en donde se registra la mayor cantidad de víctimas de casos de delitos cibernéticos, alcanzando el 34.8% del total de casos en el periodo comprendido entre noviembre del 2023 y abril del 2024; seguido por el grupo de personas que tienen entre 30 y 49 años, los cuales registraron del 30.1% del total de casos durante ese mismo periodo de tiempo; mientras que el grupo de personas que tienen de 65 años a más apenas alcanzaron el 15.2%; ello se explica porque las personas que se ubican en este rango de edad no suelen realizar actividades económicas empleando dispositivos tecnológicos. Así mismo el monto de dinero perdido por las víctimas alcanzó la cifra de 26.9 millones de dólares.

POBLACIÓN URBANA VÍCTIMA DE CIBERDELITOS EN EL PERÚ NOVIEMBRE DE 2023 A ABRIL DE 2024



Fuente: Instituto Nacional de Estadística e Informática, disponible en el siguiente enlace web:
<https://ebiz.pe/noticias/el-alto-coste-de-la-cibercriminalidad-un-especial-de-ebiz-noticias/>

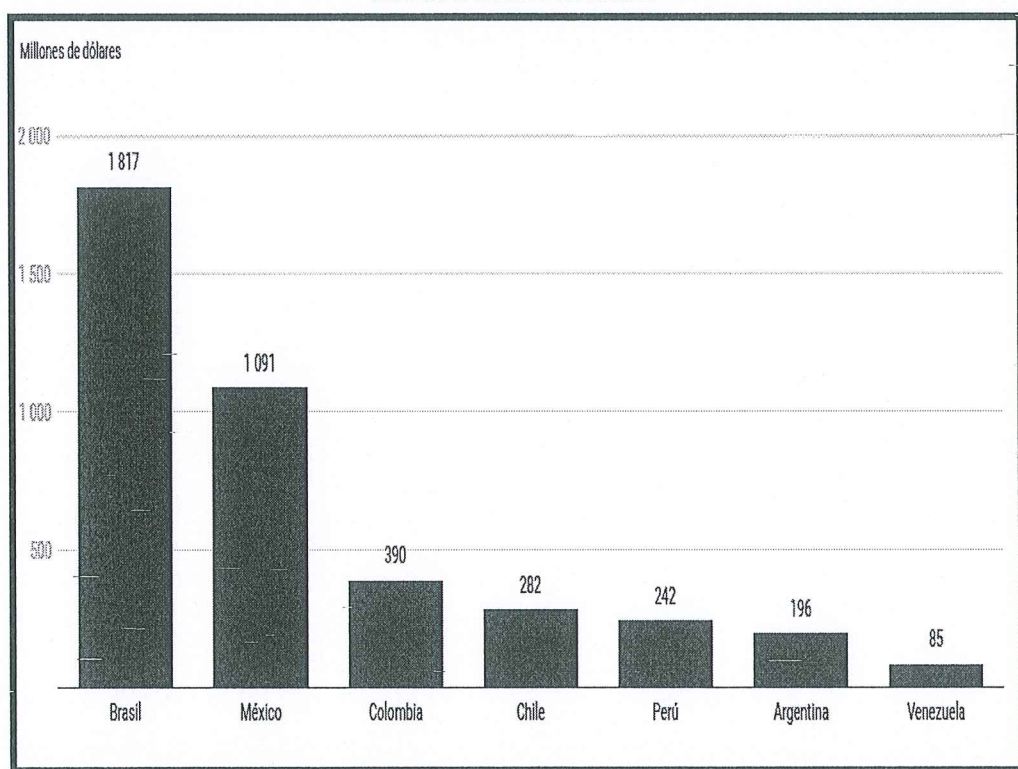


GARCÍA CORREA IDELSO MANUEL

"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"

Es necesario mencionar, que de acuerdo a lo señalado por CEPLAN⁴, Perú es uno de los países en donde lamentablemente menos se invierte en ciberseguridad en la región, alcanzando la cifra de inversión en ciberseguridad en el año 2022 el monto de apenas 242 millones de dólares, cifra muy por debajo de lo registrado en otros países como Brasil (1,817 millones de dólares), México (1,091 millones de dólares) y Colombia (390 millones de dólares); superando únicamente a Argentina (196 millones de dólares) y Venezuela (85 millones de dólares).

VALOR DEL MERCADO DE CIBER SEGURIDAD EN AMÉRICA LATINA Y EL CARIBE AL 2022



Fuente: CEPLAN. Disponible en el siguiente enlace web:
<https://observatorio.ceplan.gob.pe/ficha/tg73>

⁴ CEPLAN. (2024). Incremento de controles y riesgos en el ciberespacio.
<https://observatorio.ceplan.gob.pe>. <https://observatorio.ceplan.gob.pe/ficha/tg73>



b) Problemática con la extorsión cibernética

En el Perú, si bien existe la Ley N° 30096, Ley de delitos informáticos (la cual tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación); y además considera que se podrá hacer uso de la facultad prevista en ésta en caso existan fines extorsivos, **lamentablemente el delito de extorsión cibernética no se encuentra explícitamente penalizado, no figurando como tal en el Código Penal Peruano; lo que ha ocasionado que las cifras de incidencia de este delito se incrementen de manera desmedida con el pasar de los años, a tal punto que constituye un delito que ya viene afectando potencialmente a más de 15 mil personas por lo que urge la necesidad por establecer la presencia del delito de extorsión cibernética en el artículo 200° del Código Penal; con una pena no menor de diez ni mayor de quince años.**

c) Legislación comparada

- Estados Unidos: la extorsión cibernética es un delito federal en este país, señalado en la sección 2.261A del título 18 del Código de los Estados Unidos (U. S. Code), con penas privativas de la libertad que pueden alcanzar hasta los 20 años.
- Brasil: con la Ley 14.155/2021 la cual modifica el Código Penal de dicho país, se establecen penas más severas con respecto a la invasión de dispositivos con finalidades extorsivas; las cuales pueden oscilar entre 1 y 8 años, además de las multas, y las penas aumentan si los delitos se cometen a través de infraestructuras de servidores con sede fuera de Brasil, o si la víctima es anciana o vulnerable.
- Colombia: con la Ley 1273 de 2009, se incluyeron distintos tipos de delitos informáticos en el Código Penal, estableciendo en su artículo 195 una pena de cárcel de entre 05 y 08 años para quienes abusivamente se introduzcan en un sistema informático protegido con



medidas de seguridad, con fines económicos empleando entre ellos el chantaje.

d) Marco Jurídico

La actual **Constitución Política del Perú** promulgada en el año 1993, garantiza la libertad y bienestar de toda persona, siendo así que en su artículo 2° señala textualmente que *"toda persona tiene derecho a 1) La vida, a su identidad, a su integridad moral, psíquica y física y a su libre desarrollo y bienestar ..."*

En el año 1994 fue promulgado el nuevo **Código Penal del Perú**, y en su artículo 200° tipifica como delito penal a la extorsión, señalando a éste como *"...El que mediante violencia o amenaza obliga a una persona o a una institución pública o privada a otorgar al agente o a un tercero, de una ventaja económica indebida u otra ventaja de cualquier otra índole, será reprimido con pena privativa de libertad no menor de diez ni mayor de quince años. La misma pena se aplicará al que, con la finalidad de contribuir a la comisión del delito de extorsión, suministra información que haya conocido por razón o con ocasión de sus funciones, cargo u oficio o proporciona deliberadamente los medios para la perpetración del delito. El que, mediante violencia o amenaza, toma de locales, obstaculiza vías de comunicación o impide el libre tránsito de la ciudadanía o perturba el normal funcionamiento de los servicios públicos o la ejecución de obras legalmente autorizadas, con el objeto de obtener de las autoridades cualquier beneficio o ventaja económica indebida u otra ventaja de cualquier otra índole, será sancionado con pena privativa de libertad no menor de cinco ni mayor de diez años. ..."*

La **Ley N° 30096, Ley de delitos informáticos**, la cual fue publicada el 22 de octubre del año 2013, tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia; y así mismo en su artículo 1° señala que



se podrá hacer uso de la facultad prevista en la presente Ley al delito de extorsión.

Sin embargo, a pesar de que la Ley N° 30096, Ley de delitos informáticos, señala que en caso de delitos de extorsión se podrá hacer uso de las facultades previstas en esta misma norma, lamentablemente en esta ley no se señala textualmente a la extorsión cibernética como delito, de la misma manera que ocurre en el Código Penal (en donde tampoco se señala el delito de extorsión cibernética), por lo que éste delito no está explícitamente penalizado; ocasionando ello que la incidencia de éste delito se incremente de manera exponencial en los últimos años, pasando de 3031 casos en el año 2018 a más de 19 mil casos en el año 2023.

e) Decisión Política

Actualmente, la extorsión cibernética es un delito cuya incidencia se ha incrementado de manera exponencial en los últimos años a tal punto que 15, 616 peruanos ya han sido víctimas de este delito en los últimos 03 años y en donde se aprecia que ahora no solo los ciudadanos de a pie, sino las grandes empresas e incluso entidades públicas están siendo también víctimas de ello; por lo que esto hace necesario e imperativo la intervención del actual Congreso de la República en la aprobación de una norma que permita establecer penas privativas de la libertad para el delito de extorsión cibernética en el país.

II. IMPACTO DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

La presente Ley plantea establecer penas privativas de la libertad para el delito de extorsión cibernética; por lo que impactará directamente en el Código Penal, en su artículo 200° y en la Ley 30096, Ley de delitos informáticos, en su artículo 8°.

III. ANÁLISIS COSTO BENEFICIO

- **Costo de la norma.**

Sectores afectados. La norma no genera impacto negativo en sector económico alguno del país.

Efectos monetarios. La presente medida no tiene efectos monetarios puesto que no es una ley que incida en las decisiones de política monetaria ni muchos menos genera efectos adversos sobre las expectativas acerca del desempeño futuro de los precios de la economía nacional.

Impacto económico. La norma no impacta negativamente en el desenvolvimiento del Producto Bruto Interno del país ni en otros grandes agregados económicos.

Impacto presupuestal. La presente iniciativa generará un impacto en el presupuesto como consecuencia de la manutención de los criminales en las cárceles, puesto que el Estado anualmente destina 9,924 soles por mantener y alimentar a cada preso; aunque, este impacto es insignificante si se compara con los beneficios que representa la norma desde el punto de vista de la seguridad ciudadana en el país.

- **Beneficio de la norma.**

Sectores afectados. La presente iniciativa al permitir disminuir la incidencia del delito de extorsión cibernética, impactará positivamente en la seguridad ciudadana en el país.

Efectos monetarios. La norma al no ser una ley que incida en las decisiones de política monetaria, no genera efectos monetarios adversos ni beneficiosos para el país.

Impacto económico. Se estima de acuerdo a Forbes que el delito de las extorsiones cibernéticas en el Perú, tienen un costo de entre 10 mil y 100 mil



dólares para las empresas que sean víctimas de ello⁵. Con el fortalecimiento de la seguridad ciudadana que implica la presente norma, se verá reducido este monto de manera considerable; permitiendo a muchas de estas empresas poder gozar de mayor liquidez en su desenvolvimiento económico; lo que permitirá que todos los sectores económicos del país mantengan un crecimiento esperado.

Impacto presupuestal. Con la contribución a la seguridad ciudadana que generaría la norma, al reducirse el impacto de la actividad ilícita de la extorsión cibernética, esto permitirá al Poder Ejecutivo el destinar menos recursos para reducir las cifras de la incidencia de este delito y así gozar de mayor solvencia que permitan incrementar el Presupuesto Nacional para el siguiente periodo anual.

IV. RELACIÓN CON LAS POLÍTICAS DE ESTADO EXPRESADO EN EL ACUERDO NACIONAL

La presente norma se enmarca con la Agenda Legislativa 2024-2025, puntualmente con el Objetivo 1: Democracia y Estado de Derecho, **Política N° 7: Erradicación de la violencia y fortalecimiento del civismo y la seguridad ciudadana** y en el punto N° 18: **"Medidas en favor de la seguridad ciudadana y el civismo"**, esto porque esta política señala que el Estado se compromete a consolidar 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; que es precisamente lo que busca la presente norma, ya que al permitir reducir la incidencia del delito de extorsión cibernética; se permitirá que miles de personas que son víctimas de este delito, puedan volver a recuperar su tranquilidad y a la vez gozar de mayores recursos para sus actividades económicas.

⁵ Forbes. (2024). ¿Qué tanto han avanzado los ciberataques y qué estrategias pueden adoptar las empresas que operan en Perú para enfrentarlos? <https://forbes.pe/>.
<https://forbes.pe/especiales/2024-02-15/que-tanto-han-avanzado-los-ciberataques-y-que-estrategias-pueden-adoptar-las-empresas-que-operan-en-peru>