# UNIVERSIDAD PRIVADA SAN JUAN BAUTISTA

**FACULTAD DE DERECHO**

**ESCUELA PROFESIONAL DE DERECHO**

# LA INEFICACIA DE LA LEY 30096 DE DELITOS INFORMÁTICOS EN SU APLICACIÓN PARA EL DELITO DE CIBEREXTORSIÓN EN EL PERÚ

**TESIS**

**PRESENTADO POR BACHILLER**

**RIVAS LEÓN HERNÁN MANUEL**

**PARA OPTAR EL TÍTULO PROFESIONAL DE**

**DERECHO**

**LIMA - PERÚ**

**2021**

**ASESOR(A)**

**Dra. Alicia Asencios Agama**

# AGRADECIMIENTOS


- A la Dra. Balarezo Mares Denisse Alicia, por su apoyo brindado durante mi etapa de estudiante y egresado, así como también sus enseñanzas brindadas como docente.
- A la Dra. Asencios Agama Alicia Angélica, por su apoyo, orientación, dedicación y esfuerzo para que este proyecto de tesis cumpla con los objetivos trazados.
- A todos mis profesores de la Facultad de Derecho, por la calidad de enseñanza, los conocimientos transmitidos y el legado recibido, por sus observaciones y porque en todo momento me incentivaron a cumplir mis metas en esta carrera.

Este trabajo está dedicado a:

- A mí Padre Juan Rivas, por su apoyo, sacrificio y confianza que siempre tuvo en mí para salir siempre adelante.

- A mí Madre Olga León, por darme siempre lo mejor y guiarme siempre en todos los momentos de mi vida.

- A mis Hermanos: Juan, Javier y Maritza que siempre hemos permanecido unidos en todo momento.

# RESUMEN

El presente trabajo de tesis titulado: “La ineficacia de la ley 30096 de delitos informáticos en su aplicación para el delito de ciberextorsión en el Perú”, tiene el objetivo general de conocer la ineficacia de la ley 30096 de Delitos Informáticos, mediante sus dificultades que se presenta al aplicar la ley 30096 de Delitos Informáticos en el Perú, para combatir los ciberdelitos, siendo esto un tema actual, trascendental e importante, porque trata de explicar de manera descriptiva en base a una investigación documental, las diferentes herramientas, técnicas que utilizan los cibercriminales para cometer delitos ilícitos, que perjudican a los ciudadanos, empresas y pymes.

Se enfatiza, que el delito de ciberextorsión, es un delito grave que atenta al patrimonio, a la dignidad de las personas, siendo un sector delictivo de rápido crecimiento, innovador y rentable a nivel mundial. Es por ello analizar la ineficacia de la ley N° 30096; para combatir la ciberdelincuencia. Cabe resaltar que los convenios internaciones de cibercriminalidad también contribuyen a la regulación de las normas.

Para efecto de un mayor entendimiento, la presente investigación se ha dividido en 5 capítulos, los cuales han sido desarrollados cumpliendo los lineamientos metodológicos y técnicos establecidos.

# ABSTRACT

This thesis work entitled: "The ineffectiveness of law 30096 on computer crimes in its application to the crime of cyber extortion in Peru", has the general objective of knowing the ineffectiveness of law 30096 on Computer Crimes, through its difficulties that It is presented when applying the Law 30096 of Computer Crimes in Peru, to combat cybercrimes, this being a current, transcendental and important issue, because it tries to explain in a descriptive way based on a documentary investigation, the different tools, techniques that use cybercriminals to commit illicit crimes, which harm citizens, companies and pymes.

It is emphasized that the crime of cyber extortion is a serious crime that threatens the heritage, the dignity of people, being a rapidly growing, innovative and profitable criminal sector worldwide. It is for this reason to analyze the ineffectiveness of Law N° 30096; to combat cybercrime. It should be noted that international cybercrime conventions also contribute to the regulation of standards.

For the purpose of a better understanding, this research has been divided into 5 chapters, which have been developed in compliance with the established methodological and technical guidelines.

# INTRODUCCIÓN

La era de las comunicaciones, la materialización de la idea del mundo como una aldea global, el ciberespacio, los cibernautas, el impacto de las tecnologías de la información; han implicado una transformación en la forma de convivir en sociedad.

Dentro de este marco de transformación, el cambio producido por el mal uso de la informática ha hecho que surjan nuevas conductas merecedoras del reproche social que, sin embargo, no siempre son fáciles de tipificar. Así, han surgido modalidades delictivas relacionadas a la ciberextorsión.

La ciberextorsión ya no es un nuevo fenómeno, socialmente, ni para el derecho penal en particular. La extorsión informática o ciberextorsión ya lleva varios años de gestación, desarrollo y sobre todo de mucha práctica, bastante lucrativa para los ciberdelincuentes.

Si bien hace años que la ciberextorsión forma parte de la delincuencia en nuestra sociedad, no deja de sorprender que en la última década el índice de ciberextorsión haya aumentado notoriamente; quizás, es una problemática que, a los ojos del ciudadano común, se ha hecho cada vez más visible.

El inexorable paso del tiempo, en combinación con otros aspectos (como el aumento de la dependencia de las personas de las tecnologías de la información), se encarga de generar los incidentes de seguridad de la información que hacen que el ciudadano común vaya tomando conocimiento y dimensión de la existencia de este tipo de delito.

**ÍNDICE**

**Figuras**

**Tablas**



**Ecuaciones**

# CAPÍTULO I: EL PROBLEMA

## 1.1 Planteamiento del Problema

El accionar delictivo de los sujetos que cometen delitos informáticos, ciberextorsión, varia rápidamente a consecuencia de los cambios tecnológicos; lo que no ocurre con la norma que regula y sanciona este tipo de delitos en nuestra legislación.

Existen diversos métodos, técnicas y herramientas de cibercriminalidad que cada vez son más frecuentes y están en constante progreso por la inadecuada utilización de las TIC's (Tecnologías de Información y Comunicación) con las cuales experimentan los agentes ciberdelincuentes, originando un aumento en torno a la aparición de nuevos actos ilícitos denominados delitos informáticos en su aplicación para el delito de ciberextorsión.

## 1.2 Formulación del Problema

### 1.2.1 General

¿Qué medida se debe adoptar en el Perú para que disminuya la ineficacia de la ley 30096 de Delitos Informáticos?

### 1.2.2 Específicos

- ¿El aumento de las ciberextorsiones se debe a los métodos, técnicas, herramientas perfeccionadas y sofisticadas, que usan los grupos organizados de ciberextorsionadores?
- ¿Las herramientas logísticas de la DIVINDAT son adecuadas para que cumpla un rol importante en la lucha contra las ciberextorsiones?
- ¿Se ha reglamentado la ley 30096 de Delitos Informáticos, para que en su aplicación no exista impedimentos y transgresiones?
- ¿Los estudios, charlas de la ley 30096 de Delitos Informáticos, ha sido actualizada conforme al avance de nuevos ciberdelitos??

- ¿Se adecuado la ley 30096 de Delitos Informáticos al convenio de Budapest?

## 1.3 Justificación

El uso de la tecnología de la información desde su aparición hasta la actualidad está en aumento de manera acelerada, ya que se ha vuelto indispensable el uso del internet para las personas, de diferentes edades que necesitan estar conectadas y poder desarrollar diversas actividades.

Con la pandemia que estamos afrontando actualmente, el uso del internet a nivel mundial ha crecido en gran escala, porque se ha considerado el único medio, para que las actividades tanto de escolares como profesionales sigan desarrollándose, de manera más fácil, moderna y actualizada. Pero, así como avanza el uso de la tecnología, los ciberextorsionadores generan nuevas ciberextorsiones, que solo son contempladas de manera general en la Ley Nº 30096 de Delitos Informáticos.

Teniendo como base la Ley Nº 30096 de Delitos Informáticos, donde no se establecen con claridad los procedimientos y reglas que proceden a la investigación, juicios y sanciones relacionados con las ciberextorsiones, cometidos por ciberextorsionadores con la utilización de tecnologías informáticas o de comunicación, que atentan no solo el patrimonio, si no la integridad de sus víctimas.

Asimismo, la Ley Nº 30171 que modifica a la ley Nº 30096, con el objetivo de adecuarla al convenio de Budapest, para que en materia penal se homologuen normas de derecho penal de manera estandarizada internacionalmente para combatir los ciberdelitos.

Teniendo conocimiento que el Perú continúa afrontando ciberextorsiones desarrollados, sofisticados, especializados, de manera progresiva y

proveniente de cualquier parte del mundo por grupos organizados y que tienden a evolucionar. Y siendo una realidad problemática que no solo afecta a determinadas personas sino también a nivel social o a nivel territorial peruano. Es por eso que la presente tesis pretende precisar cuáles son los factores que determinan que la ley 30096 de Delitos Informáticos tenga poca eficacia en su aplicación en el delito de ciberextorsión en el Perú.

Conociendo que las ciberextorsiones son combatidas de manera conjunta con la División de Investigación de Alta Tecnología – DIVINDAT de la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial, pero a falta de personal con conocimientos especializados, la investigación de las ciberextorsiones se vuelve compleja.

Sabiendo que actualmente en el Perú no existen Fiscalías y Juzgados Especializados de Delitos Informáticos, que puedan combatir de manera eficientemente los ciberdelitos, especialmente las ciberextorsiones.

## 1.4 Delimitación del área de estudio

La presente tesis se delimita en analizar la ineficacia de la Ley 30096 en la prevención del delito de ciberextorsión en el Perú.

## 1.5 Limitaciones de la investigación

Las principales limitaciones que encontré para la realización del presente trabajo de tesis son la carencia de normas específicas sobre los delitos de ciberextorsión, pocos trabajos de investigaciones que hayan desarrollado investigadores sobre el delito de ciberextorsión, ya que este tema ha sido tomado en cuenta para varios investigadores de manera general como Delitos Informáticos. También he encontrado que no existe página web independiente de la DIVINDANT, en donde se pueda tener información relevante y datos actualizados de las ciberextorsiones en el Perú.

## 1.6 Objetivos

### 1.6.1 General

Conocer la ineficacia de la ley 30096 de Delitos Informáticos, mediante sus dificultades que se presenta al aplicar la ley 30096 de Delitos Informáticos en el Perú, para combatir los ciberdelitos.

### 1.6.2 Específicos

- Identificar los métodos, técnicas, herramientas perfeccionadas y sofisticadas que usan los grupos organizados de cibereextorsionadores, que han contribuido al aumento de las ciberextorsiones.
- Identificar las herramientas logísticas que utiliza la DIVINDAT.
- Investigar si existe un reglamento de la ley 30096 de Delitos Informáticos.
- Identificar actualizaciones de la ley 30096 de Delitos Informáticos, de acuerdo al avance de nuevos ciberdelitos.
- Identificar si la ley 30096 de Delitos Informáticos esta adecuada al convenio de Budapest.

## 1.7 Propósito

El propósito de la presente tesis consiste en dar una solución al problema sobre la ineficacia que se presenta en la aplicación en el delito de ciberextorsión en el Perú, de acuerdo a la Ley 30096.

Este propósito, se generó porque actualmente las ciberextorsiones sigue siendo un problema social de nuestro Perú, que lo encontramos en nuestro entorno en forma latente y cada vez en mayor escala. Es por eso que se busca contrarrestar este problema y dar bienestar a las personas que han sido ciberextorsionadas.

# CAPÍTULO II: MARCO TEÓRICO

## 3.1 Trabajos Nacionales

De acuerdo al tema de investigación: “La ineficacia de la ley 30096 de delitos informáticos en su aplicación para el delito de ciberextorsión en el Perú”, tomando como estudio de sus variables dependiente e independiente, podemos citar y detallar las conclusiones de los siguientes trabajos de investigación:

Así tenemos al tesista Morales Delgado (2016)**,** en su Tesis titulada: “La Inseguridad al utilizar los servicios de Redes Sociales y la Problemática Judicial para regular los Delitos Informáticos en el Perú-2015”, de la “Universidad Señor de Sipán”, para lograr el título profesional en derecho, el cual manifiesta en sus conclusiones:

1. En su primera conclusión el autor menciona que en los años 60s existía diversos aparatos rudimentarios que facilitaban las labores del ser humano, el cual a través de diversas generaciones han ido evolucionando hasta la aparición de las computadoras, los cuales durante cada periodo de tiempo vienen evolucionándose.
2. La segunda conclusión habla sobre las nuevas tecnologías en un mundo globalizado, lo cual implica nuevas formas delictivas, que sin una legislación que prevea estos aspectos, causaran nuevos problemas más difíciles de combatir.
3. La tercera conclusión trata sobre como el Internet ha ido evolucionando, brindando diversas aplicaciones para resolver actividades no solo laborales sino también en la comunicación, información, entre otros aspectos, convirtiéndose en una herramienta que facilita el beneficio del hombre gracias a la facilidad de su uso, y las malas intenciones de las personas.

4. La cuarta conclusión indica la influencia de los sistemas informáticos dando lugar a la existencia del Derecho Informático, enfocado en la protección de los datos informáticos y la información concentrada en medios magnéticos o digitales.
5. La quinta conclusión menciona sobre la protección de diversos bienes jurídicos en las leyes reguladoras de delitos informáticos, en las cuales, se han encontrado otras leyes contradictorias para su inadecuada inaplicabilidad; tal es el caso del delito de hurto y sus agravantes, el cual es protegido en el Código Penal.
6. La sexta conclusión habla sobre como la delincuencia ha ido en crecimiento con el uso de medios más modernos para realizar fines delictivos con el uso de las computadoras, cuya forma de combatir este delito es el establecimiento de legislaciones acorde a este problema, tanto a nivel nacional, local e internacional.
7. La séptima conclusión menciona que la problemática de la Delincuencia Informática se debe al avance de la tecnología informática reflejado en sus medios computacionales utilizados por la delincuencia; sin embargo, han aparecido en los sistemas medios de seguridad para guardar información dentro de esos sistemas informáticos denominados encriptación, sin embargo, la delincuencia se ha asistido por expertos en informática (haker, lamer y craker) para violar esa seguridad.
8. Como última conclusión menciona sobre como la delincuencia informática desde los años 70s ha generado en el mundo grandes daños a personas, empresas, entidades financieras y a los propios países. Esta delincuencia ha sido regulada internacionalmente por el Convenio de Budapest. La Convención Internacional sobre la Delincuencia Cibernética, es uno de los grandes problemas de toda clase de delincuencia, se trata de detectar el modus vivendi y operandi del delincuente, por lo que una de las ciencias auxiliares del Derecho Penal para llevar a cabo esa finalidad es la

> Criminalística, el cual, ayuda a la Policía Nacional lograr aprender a los delincuentes que utilizan los avances tecnológicos para sus fines delictivos; se oculta y huye a través de las líneas inalámbricas y alámbricas de estos sistemas computacionales (págs. 111-114).

De igual modo los tesistas Cárdenas Gallardo & Lazo Fernández (2014), en su Tesis titulada: “Delitos Informáticos y el rol de La División de Investigación de Delitos de Alta Tecnología PNP, Lima. 2013”; del “Centro de Altos Estudios Nacionales”, CAEM de Perú, para lograr el grado académico profesional de Magister de Desarrollo y Defensa, se manifiestan las siguientes conclusiones:

1. Como primera conclusión, se ha determinado mediante esta investigación que, en los delitos informáticos, el rol de la DIVINDAT - PNP es positivo, habiéndose probado nuestras hipótesis.
2. Como segunda conclusión, determina que los delitos informáticos de mayor incidencia que se denuncian a la DIVINDAT – PNP; es respecto a operaciones fraudulentas bancarias con violación de accesos de claves secretas a través de la “banca en línea” o “banca por internet” y clonaciones de tarjetas de créditos y tarjetas de débitos.
3. La tercera conclusión, respecto al espectacular desarrollo de las TIC’s, abren mayores posibilidades de delincuencia, como son los delitos informáticos, constituyendo la red de internet como nueva vía de comunicación, el instrumento o herramienta tecnológica más utilizada en la comisión de estos delitos, en razón que los delincuentes consideran su fácil acceso, menor riesgo y el anonimato que les ofrece.
4. Como última conclusión, la DIVINDAT – PNP, actualmente tiene déficit en su personal, tanto en número como en personal experto, no tienen los instrumentos tecnológicos suficientes, que les permitan estar a la par de las Unidades similares del extranjero, y

que pone en riesgo el cumplimiento eficiente y eficaz de la misión asignada (págs. 127-128).

Igualmente, para el tesista Morí Quiroz (2019) en su Tesis titulada: “Los Delitos Informáticos y la Protección Penal de la intimidad en el Distrito Judicial de Lima periodo 2008 Al 2012” de la “Universidad Nacional Federico Villarreal”, Lima, Perú, para obtener el grado académico profesional en Maestría de Derecho Penal”, se manifiestan las siguientes conclusiones:

1. Como primera conclusión, se da a conocer la situación de la labor de los jueces que aceptan que existe ausencia y desconocimiento de la tecnología de la información en la investigación y juzgamiento de los delitos informáticos, y la protección penal de la intimidad, pero son indiferentes para los fiscales y junto a los policías dicen estar en desacuerdo.
2. La segunda conclusión, expresa que los jueces y fiscales aceptan que hay transgresiones de las legislaciones vigentes. Los jueces están de acuerdo con la determinación del tipo penal, mientras que los policías y los fiscales están en desacuerdo.
3. En la tercera conclusión, los jueces están de acuerdo con la inadecuada determinación del daño, con el insuficiente cálculo del monto indemnizatorio, mientras que los policías y fiscales, son indiferentes y están en desacuerdo.
4. En la cuarta conclusión, se manifiesta que, ante el trabajo de los operadores de justicias, hay que defender la intimidad, con independencia de la finalidad perseguida por las conductas de los criminales.
5. En la quita conclusión, se determina que para los operadores de justicia existe la deontología tecnológica, que influye en la impropia determinación del tipo penal, la competitividad de la investigación y el juzgamiento de los delitos informáticos en la protección penal contra la intimidad.

6. Como sexta conclusión, se menciona que los jueces están de acuerdo en una especialización de los operadores de justicia sobre delitos informáticos para favorecer el desarrollo sobre el acuerdo de una inadecuada determinación del daño causado.
7. Como séptima conclusión, los jueces y policías están de acuerdo que los operadores de justicia están bien preparados para pronunciarse eficazmente sobre la responsabilidad civil en sede penal sobre la responsabilidad del criminal (págs. 72-73).

Del mismo modo el tesista Cotrina Yucra (2018) en su Tesis titulada: “Los factores principales que impiden la aplicación de la Ley N° 30171- Lima Norte en el año 2016” de la “Universidad César Vallejo”, Lima, a fin de obtener el título académico profesional en Derecho, se manifiestan las siguientes conclusiones:

La finalización del trabajo o investigación son las conclusiones en donde el tesista o investigador indica lo más importante de todo el trabajo, indicando la afirmación o negación de las hipótesis investigadas.

En el presente trabajo de investigación, en la etapa final de todo el desarrollo de la tesis, se llegó a conseguir el objetivo general y los específicos planteados, que estos a su vez han ayudado a fundamentar los supuestos jurídicos general y los específicos, planteados en el primer capítulo, en ese contexto se ha podido concluir lo siguiente:

1. En la primera conclusión, los factores principales que han impedido la aplicación de la Ley Nº 30171 han sido: la falta de capacitaciones a los magistrados, fiscales y PNP y la falta de cooperación operativa, la cual se podría lograr mediante la adhesión al Convenio de Budapest.
2. En la segunda conclusión, la falta de capacitación de los magistrados, fiscales y PNP, es un factor principal que impide la

correcta aplicación de la Ley Nº 30171, ya que las capacitaciones a estas autoridades no bastan con hacerlas a la ligera, sino que se debe realizar con asistencia profesional de expertos que sepan de estos asuntos y con el material necesario, en la quinta disposición complementaria final no derogada de la Ley Nº 30096, nos habla del tema de las “Capacitaciones”, pero lamentablemente se verifica en la práctica que difícilmente se viene aplicando, ya que en dicha disposición las capacitaciones mencionan que son un deber realizarlas, mas no brinda un carácter de obligación a las instituciones públicas encargadas.

3. En la tercera conclusión, la falta de adhesión al Convenio de Budapest es un factor principal que impidió la correcta aplicación de la Ley Nº 30171 o también llamado al convenio Internacional de Cibercriminalidad, los expertos consultados mencionan que no ser partícipe de dicho convenio es un factor que puede retardar el proceso de captura y sanción a los delincuentes informáticos, además es muy importante la cooperación internacional que este convenio nos podría generar (pág. 91).

Por último, el tesista Tenorio Pereyra (2018) en sus Tesis titulada: “Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia”, de la “Academia Diplomática del Perú: Javier Pérez de Cuellar”, para obtener el grado académico profesional de Master en Diplomacia y Relaciones Internacionales, manifiesta las siguientes conclusiones:

1. En la primera conclusión, los ciberdelitos y las modalidades como se realizan estos tipos de delitos informáticos se encuentran en constante evolución desde la masificación del Internet a inicios de la década de los 90, generando pérdidas económicas y daños sociales cada vez mayores gracias al uso de nuevas tecnologías y software para la comisión del delito desde cualquier punto del

planeta y en cualquier momento. Para protegerse de los ciberdelitos, instituciones y empresas están realizando inversiones en ciberseguridad, generando más pérdidas económicas reflejadas en menores ingresos y posibles déficits proyectados, y no haciendo frente al principal problema, el cual dejó de ser un exclusivo de un país, para ser un problema que debe ser combatido por todos los Estados mediante la cooperación internacional en materia jurídica, de conocimientos, experiencias e información relevante para establecer responsabilidad penal a los involucrados.

2. En la segunda conclusión, el Convenio de Budapest sobre la Ciberdelincuencia es una herramienta de gran utilidad en materia de derecho penal sustantivo y procesal para todos los Estados Parte al buscar la una política penal común ante los ciberdelitos, y el incrementar las capacidades y eficiencia en la investigación, persecución y proceso penal. Un factor adicional que deben considerar los Estados que deseen adherirse es la cooperación internacional, tanto en materia judicial y para la reducción de las brechas de conocimientos y tecnología, lo que permitirá un mejor accionar ante diferentes situaciones. Los avances en el proceso de adhesión varían entre cada Estado, en el caso de América Latina y el Caribe, son pocos los Estados adheridos o que están en fase avanzada de adecuación para su adhesión.
3. En la tercera conclusión, el Estado peruano ha desarrollado una legislación interna relacionada a los delitos informáticos y ciberdelincuencia, que se adecúa y supera los estándares requeridos por el Convenio de Budapest sobre la Ciberdelincuencia. Para ampliar su margen de acción, y obtener cooperación y acceso a información de importancia para la persecución del delito, inició el proceso de adhesión al Convenio, proceso que lleva más de 3 años y cuya invitación está próxima a

vencer. Tras la adhesión, el Perú asumirá responsabilidades que deberá cumplir, pero para lograrlo deberá fortalecer a instituciones como el Ministerio de Relaciones Exteriores, Ministerio de Justicia y Derechos Humanos y el Ministerio Público. Este fortalecimiento debe conseguir reducir las brechas tecnológicas que tiene cada institución del Estado y agilizar los procesos internos para responder adecuadamente ante solicitudes de otros Estados Parte. De igual manera, se deberá aprovechar las opciones disponibles en el Convenio para captar cooperación internacional, y adecuarnos correctamente a los constantes cambios en el ciberespacio y combatir a los ciberdelitos que evolucionan constantemente (págs. 94-95).

### 3.2 Trabajos Extranjeros

Tenemos al tesista Mateos Pascual (2013)**,** en su Tesis titulada: "Ciberdelincuencia Desarrollo y persecución tecnológica", de la "Universidad Politécnica de Madrid", España, para optar el título profesional de Telemática, manifiesta las siguientes conclusiones:

1. En su primera conclusión habla sobre la ciberdelincuencia de cómo esta supone una nueva visión de lo que hasta ahora se había considerado como acto delictivo. Donde los delincuentes han encontrado durante las 24 horas conectados a la red un nuevo lugar, lleno de posibilidades, donde asechar y cometer sus delitos.
2. La segunda conclusión se menciona sobre la delincuencia tradicional, el ciberdelincuente no posee un único perfil, se pueden diferenciar numerosos tipos según sea su metodología, objetivos personales y papel en una estructura criminal organizada.
3. La tercera conclusión menciona que tanto las organizaciones, gobiernos y ciudadanos se encuentran expuestos a todo tipo de delitos y estafas en la red, no siempre como papel de víctimas. En

ocasiones el anonimato y libertad obtenida de internet lleva al límite entre lo legal y lo ilegal.

4. La cuarta conclusión habla sobre los métodos y técnicas utilizadas por los ciberdelincuentes para alcanzar sus objetivos; en la cual se puede definir un análisis de su motivación principal a la que estos ciberdelincuentes son guiados. Primeramente, su objetivo principal es obtener rentabilidad económica como fruto de sus actos. Para ello utilizan métodos de estafas y robos de información, y sus principales técnicas de acceso a sus víctimas son mediante correos electrónicos y sitios web's, para luego dar paso al uso de las redes sociales y terminales móviles de última generación.
5. La quinta conclusión menciona sobre la aparición de los denominados ciberdelincuentes sociales formados por grupos de individuos cuyos delitos afectan directamente a las personas en su integridad física y psicológica.
6. En la sexta conclusión, es donde se menciona sobre la aparición de grupos organizados llamados ciberdelincuencia ideológica. Estos grupos utilizan nuevas herramientas tecnológicas y los conocimientos informáticos necesarios para desacreditar a sus víctimas y mostrar sus ideales. Ante estos actos de rebeldía o amenazas, los gobiernos, no dudan en denominarlos como Ciberterroristas a aquellos que atentan contra sus sistemas, su reputación, infringen sus leyes y derechos que restringen su uso y acceso libre a determinada información.
7. Como séptima conclusión, se remonta al pasado de aquellos jóvenes que decidieron saltarse las normas para investigar y seguir a los avances tecnológicos. Dejando en duda, que hubiera pasado, si los sistemas informáticos, redes de la información hubieran sido protegidos y regulados por sus creadores de acuerdo a ley.
8. La octava conclusión, realiza un análisis sobre el pasado, presente y futuro de la ciberdelincuencia, el cual, sitúa sus objetivos en el

ciberespionaje, la ciberguerra, y el crecimiento de las infecciones en los terminales móviles y redes sociales, generándose un aumento de ataques en los servicios de la Internet.

9. Como novena conclusión, ya identificado la gravedad y la dificultad, se plantea un análisis de las diferentes soluciones y medios existentes para combatir el problema del cibercrimen. En primer lugar, la educación ciudadana y la concienciación sobre el peligro potencial que esto supone en el manejo de información confidencial como medida básica de prevención y lucha contra la ciberdelincuencia. El ciberdelincuente basa sus argumentos y métodos en la ingeniería social y el engaño, lo cual, se vuelve para ellos más complejo si sus víctimas ya se encuentran preparadas.
10. Como decima conclusión, señala la aparición del Convenio sobre cibercriminalidad firmado en Budapest en 2001, en donde los gobiernos establecen acuerdos internacionales, como medida fundamental para garantizar la seguridad de los ciudadanos y las organizaciones, y castigar a aquellos que lo infrinjan.
11. En la onceava conclusión, se manifiesta sobre la instalación y adopción de medidas de seguridad para los usuarios y las organizaciones ante la vulnerabilidad que presentan los sistemas de información y las comunicaciones que cada vez se torna más peligroso, y no caer ante innumerables estrategias de los ciberdelincuentes se ha convertido en una tarea prácticamente imposible. Estas medidas han conseguido que sus esfuerzos vayan dando sus frutos y que, cada vez con mayor eficacia puedan luchar contra la ciberdelincuencia (págs. 151-152).

Así mismo los tesistas Aguirre Linares & Sevillano Flores (2017)**,** en su Tesis titulada: “Desafíos a enfrentar en la Aplicación de Leyes sobre Delitos Informáticos en el Salvador”, de la “Universidad Don Bosco del Salvador”, El Salvador, para optar los títulos profesionales de Maestros en Seguridad y

Gestión Informáticos, manifiestan las siguientes conclusiones:

1. El Salvador está realizando sus primeros pasos en investigación y sanción de los delitos informáticos, y es necesario que se desarrolle, mejore e implemente mecanismos que permitan que dichas investigaciones se desarrollen dentro de los marcos regulados, controlados y mediante el uso de tecnología apropiada.
2. Los peritos informáticos presentan las siguientes habilidades: Habilidad de emitir criterios y opiniones sustentadas tanto en la parte técnica como científica, capacitación continua y secreto profesional.
3. Las estrategias que se llevan a cabo para la investigación de los ciberdelitos son: diagnóstico de la actividad delictiva, adopción de leyes y principios en materia del ciberdelito, vinculación de la Red de emergencia de contactos sobre ciberdelitos y la utilización de métodos para la recolección de evidencias(págs. 67-68).

De igual modo la tesista Ruiz Cruz(2016) en su Tesis titulada: “Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos”, de la “Universidad Nacional de Loja”, Loja, para optar el título profesional de Abogada, manifiesta las siguientes conclusiones:

1. Actualmente la comunicación de las personas por medios informáticos y de comunicación, ha contribuido a su avance, así mismo ha permitido el avance de los delitos informáticos.
2. Debe ser considerada para precauterlar, la necesidad de tipificar y sancionar los ciberdelitos para proteger la integridad e intimidad de los ecuatorianos.
3. En varias ocasiones los ciberdelitos no solo afectan a una persona, sino también a la colectividad en general.
4. De los resultados obtenidos, existen vacíos legales en la tipificación de los ciberdelitos como la apropiación de la

información y la intimidad persona en redes sociales, lo cual se debe considerar un acto antijuridico y ser causa de sanción.

5. Las redes sociales son plataformas que permiten compartir información y permite comunicarse, a la vez es un medio para cometer ciberdelitos, que son complicados para determinar el responsable del ciberdelito.
6. La falta de conocimientos tecnológicos y comunicación, es la causa para que los ejecutores de justicia cibernética, haya obviado algunos elementos que deberían incluirse en la legislación ecuatoriana (págs. 93-94).

Así mismo el tesista Montañéz Parraga (2017) en su Tesis titulada: “Análisis de los Delios Informáticos en el actual Sistema Penal Colombiano”, de la “Universidad Libre de Colombia”, Bogotá, para optar el título Profesional de Derecho, manifiesta las siguientes conclusiones:

1. Colombia ha hecho el esfuerzo de crear la ley 1273 de 20119, lo cual fortalece el tratamiento jurídico digital de la información, pero existe vacíos que puede generar contradicciones y errores al interpretar la ley.
2. Las personas que trabajan en sistemas de acuerdo al artículo 269D, indica que el que sin ser facultado destruye, dañe, borre, deteriore, altere o suprime datos, comete Daño informático, si los operadores de sistemas cometen algún error, de acuerdo al artículo en mención, el empleador puede realizar un proceso penal. De igual modo si una persona cambia la contraseña de su wifi, de acuerdo al artículo 269A, sobre acceso abusivo a un sistema informático, podría incurrir a un delito, porque estaría ingresando a un sistema informático. De acuerdo a esto, se puede generar conflicto en la interpretación de la ley y posibles errores para su interpretación de la ley y ejecución.

3. Falta un gran camino por recorrer para que los abogados tengan mayor interés aprender sobre la ley que tutela como bien jurídico la información y los datos; así como los profesionales de sistemas o telecomunicaciones que si están interesados.
4. La tecnología va evolucionando a pasos agigantados, por lo que el derecho debe ir a la par con estos cambios, y también la ley 1273 de 2009 tiene que ir cambiando y evolucionando para enfrentar nuevos retos y nuevos fenómenos sociales(págs. 81-82).

Por último, los tesistas Chavarría Pérez, Jirón Vargas, & Miranda González(2016) en su Tesis titulada: “La ciberdelincuencia y su regulación jurídica en Centroamérica con énfasis en Costa Rica, El Salvador y Nicaragua”, León, Nicaragua, de la “Universidad Nacional Autónoma de Nicaragua UNAN-León”, para optar el título Profesional de Derecho, manifiestan las siguientes conclusiones:

1. Con mayor frecuencia se presentan los delitos informáticos, afectando los derechos constitucionales de las cibervíctimas, por los ciberataques.
2. El avance tecnológico y las formas de comisión de ciberdelitos, no deben estar separadas de las reformas y creaciones legales.
3. El escaso datos sobre la cantidad real de los ciberataques, hacen difícil conocer su magnitud e impacto económico.
4. En Centroamérica, Colombia fue el primer país que regulo los delitos informáticos, mediante la Ley 9048, aprobada el 6 de noviembre 2012, incorporando nuevos tipos penales, y penas para aquellos que cometen ciberdelitos.
5. En la República de El Salvador, la ley que sanciona a los delitos informáticos, en cuanto a sus penas no ha cambiado mucho en comparación con las demás normativas como el código penal, ley de acceso a la información pública, entre otros. Las penas de dichos delitos, igual que la ley oscilan entre los 4 y 12 años, y en

caso agravante puede aumentar la tercera parte de la pena, del delito que se impute.

6. En cuanto a su método de aplicación de la ley, El Salvador tiene dificultades en dar seguimientos a los ciberdelincuentes por la complejidad de los delitos.
7. Nicaragua regula los delitos informáticos por medio de diferentes leyes, ya que no cuenta con una normativa concreta especializada en cibercriminalidad.
8. Todos los esfuerzos serán insuficientes si no se crea un instrumento regional en Centroamérica, en donde involucre a los países centroamericanos, ya que la ciberdelincuencia es transnacional (págs. 95-96).

## 3.3 Base teórica

### 1. Delitos Informáticos

Para conceptualizar que es delito informático, se debe definir que es un delito, en donde las conductas pasan a ser catalogadas como hechos ilícitos. Como indica el código penal peruano, “Son delitos las acciones u omisiones dolosas o culposas penadas por la ley.”(Ministerio de Justicia y Derechos Humanos, 2015).

La dogmatica juridico penal, considera al delito como una conducta tÍpica, antijurÍdica y culpable; cabe precisar que un acto u omisión posiblemente es típica; un acto u omisión típica posiblemente es antijuridica; que un acto u omisión antijuridica posiblemente es culpable.

Despues de haber conceptualizado que es un delito, se definirá que es un delito informático. Se entiende por delitos informáticos:

> Aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas

> típicas que únicamente pueden ser cometidas a través de la tecnología. En un sentido amplio, comprende a todas aquellas conductas en las que la Tecnología de la Información y Comunicación (TIC) son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos.(Villavicencio Terreros, 2014, págs. 286-287).

La conceptualizacion del delito informáticosegún su conducta, son típicas y atípicas; "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y las conductas atípicas son las "actitudes ilícitas en que se tienen a las computadorascomo instrumento o fin"(Telléz Valdéz, 2009, pág. 188).

La vinculación de los delitos informáticos se relaciona:

> Con la idea de la comisión del crimen a través del empleo de la computadora, internet, etcétera; sin embargo, esta forma de criminalidad no solo se comete a través de estos medios, pues éstos solo son instrumentos que facilitan, pero no determinan la comisión de estos delitos.(Mazuelos Coello, Juan, 2007, pág. 40).

Para Mühlen citado por el escritor Mazuelos Coello, Juan(2007), el delito informático, "comprende todo comportamiento delictivo en el que la computadora es el instrumento o el objetivo del hecho"(pág. 41).

Todas estas conceptualizaciones se refieren a las conductas clásicas penales; conductas ilicitas, que tienen como instrumento a la computadora para realizar el hecho delictivo y que se encuentra de forma indirecta o directa con sistemas, redes y procesamiento de datos electrónicos.

## 2. Delito de Ciberextorsión

El delito de ciberextorsión, está relacionado con el delito clásico penal de la extorsión con el uso de medios informáticos más actualizados, modernos y de fácil operatividad para los ciberextorsionadores.

Para comprender mejor que es la ciberextorsión, se conceptualizará la extorsión:

La extorsión es la "presión que se ejerce sobre alguien mediante amenazas para obligarlo a actuar de determinada manera y obtener así dinero u otro beneficio"(Real Academia Española, 2020), constituyéndose un delito "contra el patrimonio, donde el agente obliga al sujeto pasivo a entregar una cosa, suma de dinero o documento, por medio de violencia, intimidación o secuestro, con el objeto de obtener para sí o para un tercero un provecho ilícito".(Ezaine Chavéz, 2000, pág. 872).

Algunos autores tienen su propia concepción, lo definen como "una usurpación o despojo, por la fuerza, de una cosa perteneciente a otro" (Cabanellas de Torres, 2008, pág. 713) , obteniendo como "resultado complejo de dos tipos simples: un atentado a la propiedad cometido mediante el ataque o lesión a la libertad personal". (Roy Freyre, 1974, pág. 250).

Cabe resaltar que la extorsión como delito "está constituido por un ataque violento o intimidatorio destinado a que otra persona haga algo concreto, que es realizar u omitir un acto jurídico perjudicial para su patrimonio o para el de un tercero"(Quinteros Olivares, 2016, pág. 472), siendo la extorsión "un ataque a la propiedad cometido mediante un ataque a la libertad".(Creus & Buompadre, 2007, pág. 487).

Se puede concluir de manea Jurídica que el delito de la extorsión es un perjuicio patrimonial que se obtiene por medio de amenazas u

intimidación para alcanzar un lucro ilícito, en donde se aprecia los medios por medios de comisión la intimidación de la víctima que es el sujeto pasivo, alcanzada por las amenazas contra sus propiedades, daños graves a familiares o la víctima y ordenes de entrega de dinero por parte del agresor, que es el sujeto pasivo. En resumen, este delito es perjudicial tanto para los bienes económicos, como para el bienestar de los ciudadanos.

Después de tener una concepción más clara sobre el delito de la extorsión, se conceptualiza la ciberextorsión:

> El delito de ciberextorsión consiste en el uso de violencia o intimidación, aplicada a través de los medios informáticos, de manera que se consiga que la víctima realice un acto en perjuicio propio o ajeno, tramitado a través de la web. El infractor y la víctima no tienen contacto directo más allá del realizado por las redes.(Tecnología clic, 2020).

Según expertos en la materia, definen a la ciberextorsión como “una forma de chantaje que sufre la víctima de un ataque informático, mediante el cual se le fuerza a pagar para evitar sus efectos” (Panda Security, 2016, pág. 5); por lo que se considera como un delito: “invisible, que se puede cometer sin gran infraestructura, es un delito que no tiene que cometerse en la calle y es un delito que no se ve porque además las personas no saben exactamente de qué tamaño es la amenaza”.(Fundación Heinrich Böll México y El Caribe, 2013).

> La ciberextorsión, al igual que la extorsión telefónica, se inserta en los tipos de delincuencia a distancia. Incluso puede traspasar las fronteras nacionales y ser cometida desde otros países. De la misma manera, en esta modalidad podemos encontrar desde amenazas, engaños, problemas o actualización de datos

> personales de nuestras cuentas bancarias, hasta la suplantación de identidades de una página institucional o empresarial. Se trata de una práctica conocida como phishing. (Pérez Morales, Veléz Salas, Rivas Rodríguez, & Vélez Salas, 2015, pág. 119).

Se puede decir que la ciberextorsión es un conjunto de conductas delictivas como las ciberamenaza, secuestro de datos personales e información, bloqueos de sistemas operativos, otras conductas que conducen a la víctima a realizar transferencias económicas, teniendo un gran impacto en la pérdida patrimonial, afectándolos psicológicamente, por grupos de cibercriminales organizados, constituyéndose en un delito informático de gran alcance mundial.

## 3.4 Marco conceptual

### 1. Características de la Ciberextorsión

Para tener una idea más clara de las características de la ciberextorsión, se resume las principales características de los Delitos Informáticos que propone Telléz Valdéz (2009) que son:

- Son conductas cibercriminales por personas con ciertos conocimientos informáticos.
- Ocasionan pérdidas económicas, en algunas ocasiones con cifras elevadas.
- Tienen facilidades en el espacio, tiempo y lugar, ya que se puede realizar en segundos, sin necesidad de la presencia física.
- Presentan dificultades para ser comprobadas.
- Son mayormente intencionales o dolosos, en algunos casos son imprudenciales o culposos.
- Tienden a incrementar cada día más. (págs. 189-190).

Estas características que indica el autor, señalan que los ciberdelincuentes tienen conocimientos informáticos, que lo emplean de tal manera, que no sean identificados sus ataques por sus posibles cibervíctimas. Así mismo indica que los ciberdelitos afectan de manera económica, en cualquier momento, lugar, con la utilización de medios electrónicos.

Las características antes mencionadas sobre los delitos informáticos, también se relacionan con las ciberextorsiones. Otras características que se puede presentar en las ciberextorsiones en el Perú son:

- Dificultad para identificar a los ciberextorsionadores, en el mundo virtual, porque los ciberextorsionadores, usan softwares para borrar sus rastros, lo cual origina el desconocimiento del sujeto activo para sancionar penalmente la ciberextorsión.
- Poseen un grado elevado de Complejidad Tecnológica, usando softwares modernos, y en algunos casos difíciles de detectar por especialistas en ciberextorsiones.
- Obstáculo para reunir las pruebas probatorias porque por la Complejidad Tecnológica, no existe pautas estandarizadas para realizar la acumulación de las pruebas.

Estas características de las ciberextorsiones que se presenta en el Perú, es porque no existe medidas preventivas que se adelanten a una ciberextorsión moderna, actual y evolucionada. Así mismo cabe precisar que la ley Nº 30096 de Delitos Informáticos previene y sanciona los delitos informáticos, pero estas prevenciones no se han adecuado con el avance de la tecnología, ni con los estándares al convenio de Budapest.

## 2. Elementos de la Ciberextorsión

En el delito de la Ciberextorsión participan 4 elementos:

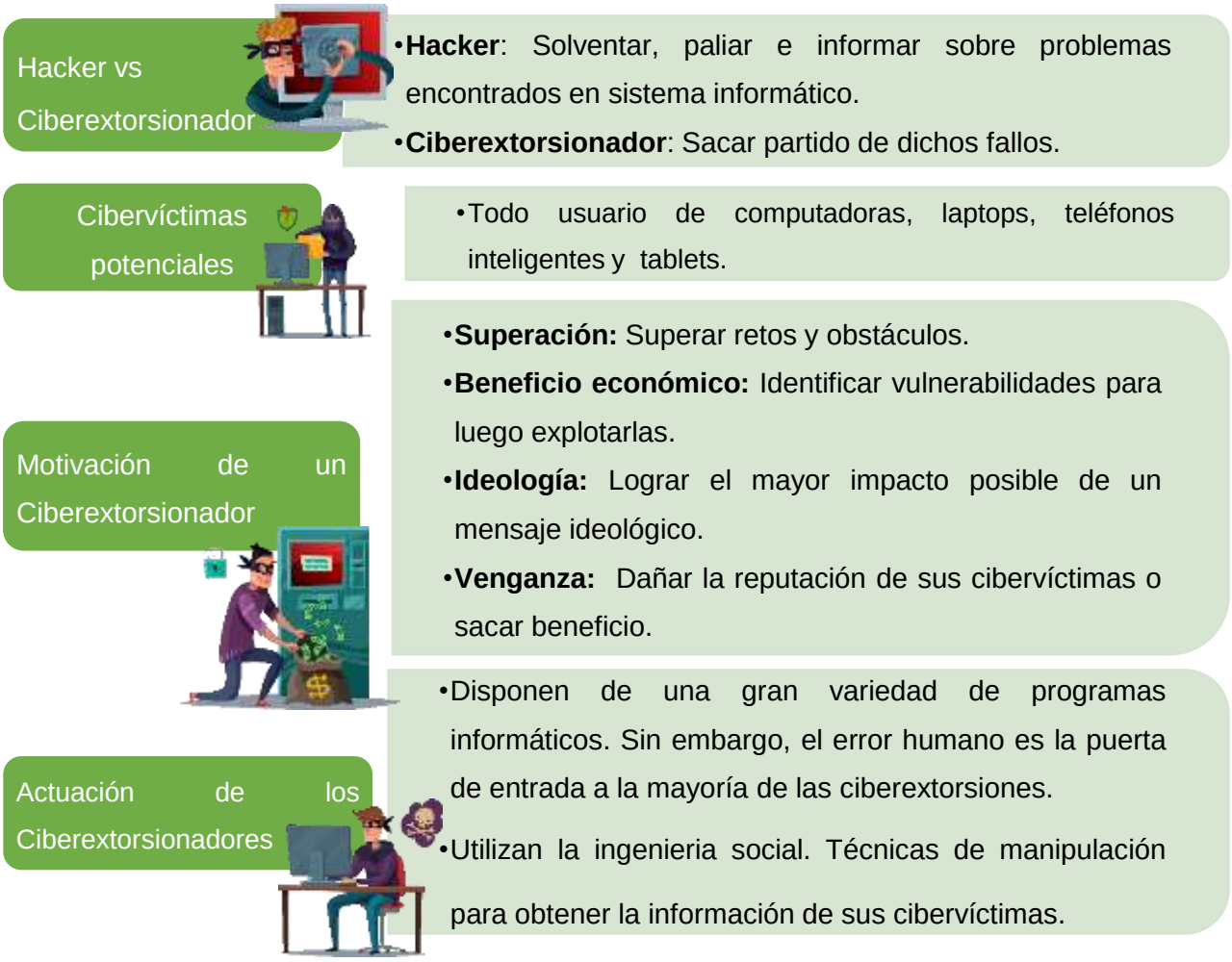
### a. Ciberextorsionadores

Son personas u organizaciones de ciberextorsionadores, con conocimientos en informática, programación, capaces de crear, desarrollar softwares maliciosos, para cometer la ciberextorsión por medio de ciberamenazas y obtener el cobro de la ciberextorsión.

Las organizaciones ciberextorsionadoras están conformadas por tres o más ciberextorsionadores, cuentan con una estructura organizacional para dividirse las tareas ciberextorsionadoras, empleando la Ingeniería Social, cuenta con una larga lista de posibles cibervíctimas que comienzan a contactarlas en los diversos países para realizar las ciberextorsiones. El monto de la ciberextorsión varía de acuerdo a la cibervíctima.

**Figura 1**

*Los extorsionadores y su actuación*




Nota: La actuación de los ciberextorsionadores frente a sus cibervíctimas. Adaptada de (Oficina de Seguridad del Internauta, 2018) y (Macrovector, Internet hacker security composition set Free Vector [Imagen], Sin fecha).

**b.Cibervíctimas**

Una potencial cibervíctima es todo usuario de computadoras, laptops, teléfonos inteligentes y tablets. Habitualmente la cibervíctima cae por engaños, por medio de correo SPAM que lo traslada a un sitio que contiene el código malicioso, que realiza el

ataque. La cibervíctima es obligada a pagar la ciberextorsión para rescatar por medio de una clave cifrada su información o sistema.

**c.Medios Informáticos de la Ciberextorsión**

La ciberextorsión es uno de los delitos con mayor ocurrencia, y hoy en día los ciberextorsionadores la practican a través del internet, redes sociales y mensajería instantánea.

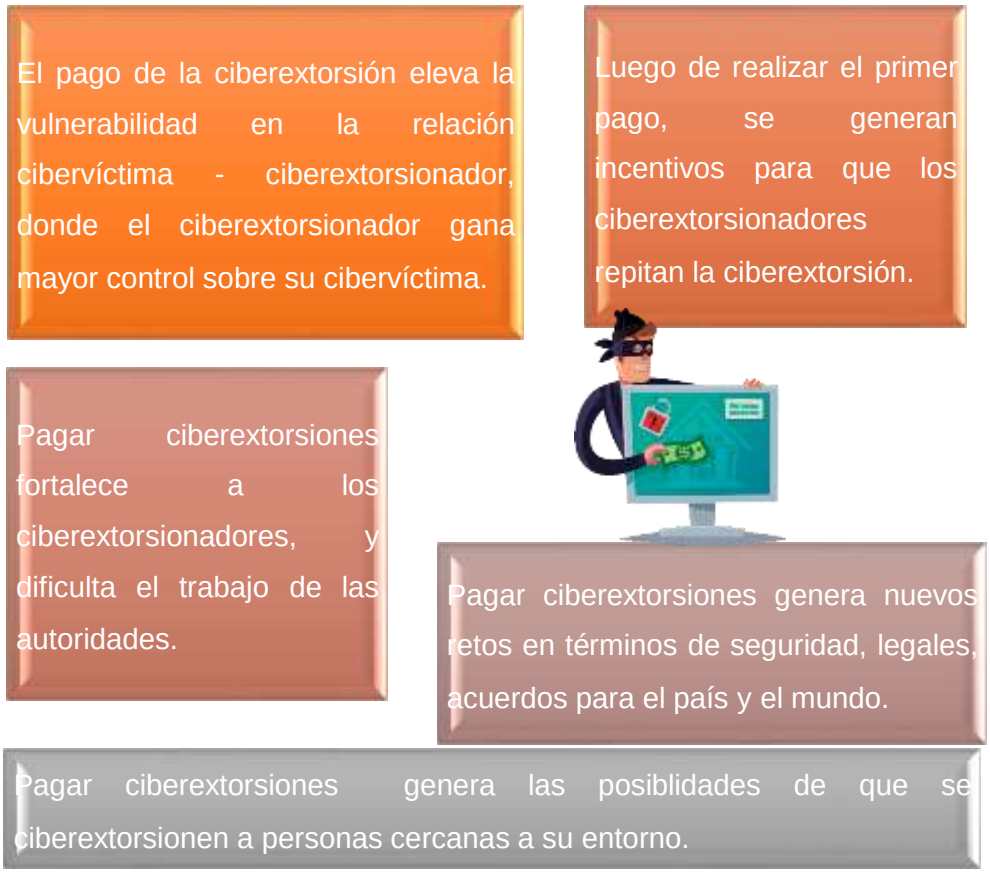
**d.Pagos de la Ciberextorsión**

El pago permite que se eleven los niveles de efectividad de la ciberextorsión, se amplíe la motivación de los ciberextorsionadores y el entorno comience a ser afectado de manera general y sistemática por la ciberamenaza de nuevas ciberextorsiones, no sólo para las víctimas sino para las que se encuentran en su entorno. Al ceder una vez, se envía un mensaje claro a los ciberextorsionadores de que pueden sacar provecho, lo que aumenta considerablemente la posibilidad de que el hecho se repita nuevamente en el futuro.

En este sentido, el pago de la ciberextorsión es un hecho que afecta la seguridad de quién la paga porque:

**Figura 2**

*Pagos de la Ciberextorsión*




Nota: Pagar ciberextorsiones genera distintas situaciones en la cibervíctima, familia, en la sociedad. Adaptado de (Fundación Ideas para la Paz, 2012) y (Macrovector, Internet hacker security composition set Free Vector [Imagen], Sin fecha).

## 3. Inversión en el delito de Ciberextorsión

Se nota un gran cambio en la inversión que realizan los ciberextorsionadores en la ciberextorsión con respecto a la extorsión.

La ciberextorsión se realiza en el mundo virtual, con herramientas como las TICS, y utilización de las redes sociales por medio del internet, en cambio en la extorsión se realiza en el mundo real, utilizando como

herramientas armas de fuego, u otras armas que perjudiquen la vida de su víctima.

La ciberextorsión, su organización es de 3 o más personas que realizan las mismas actividades, en cambio en las extorsiones es una organización criminal aproximadamente de 6 a más personas, cumpliendo cada una actividad diferente.

En la ciberextorsión la inversión es baja, ya que la ciberextorsión lo realizan de manera rápida y lo pueden realizar por medio de cabinas de internet, en cambio en la extorsión, el costo de la inversión es más elevado por su planificación y ejecución.

**Figura 3**

*Inversión en el delito de la ciberextorsión*

Nota: La inversión en el delito de la ciberextorsión es muy poca en comparación con el delito de la extorsión. Adaptado de (Del Castillo Vidal, 2011).

## 4. Métodos, Técnicas y Herramientas de los Ciberextorsionadores

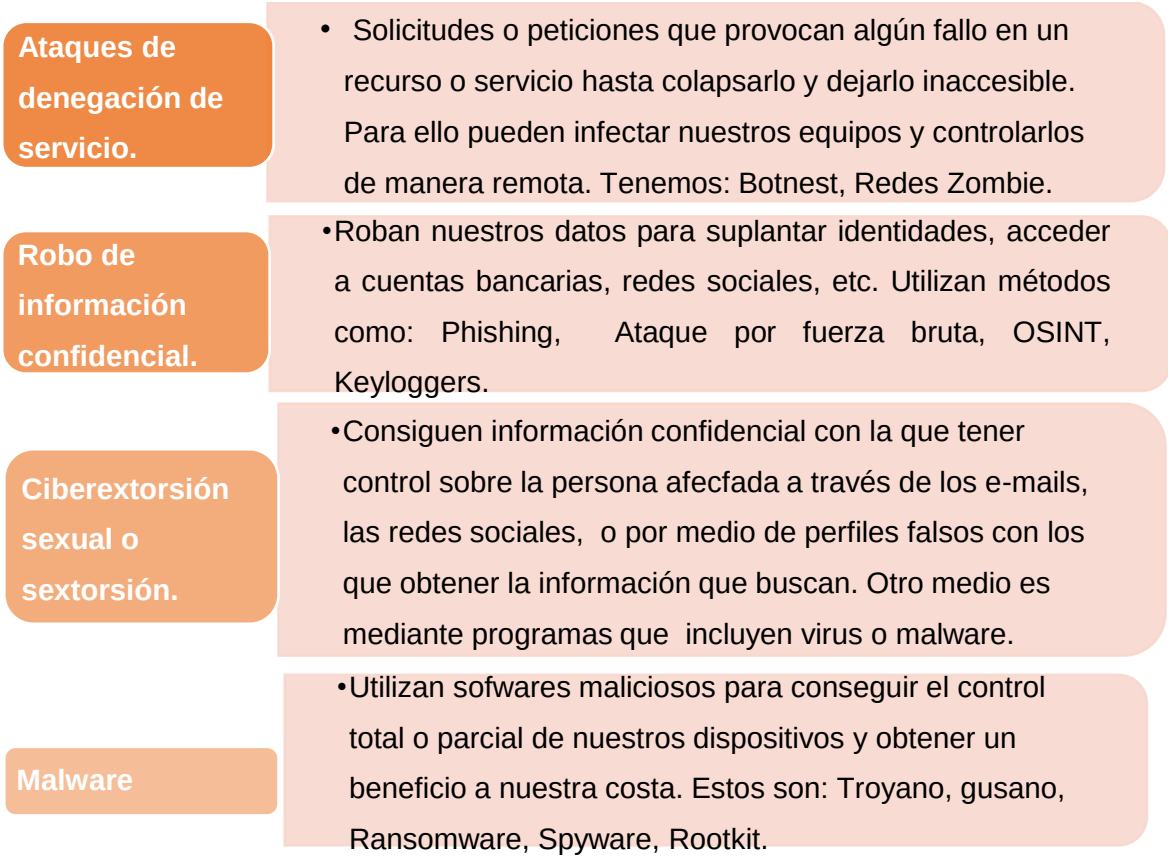
Con el avance de la tecnología, los Grupos Organizados de Ciberextorsionadores, han perfeccionado, sofisticado de manera creativa las distintas formas de cometer sus ciberextorsiones, adoptando sus enfoques estratégicos, seleccionando mejor a sus cibervíctimas, aprovechan las nuevas tecnologías, reinventan la ingeniería social, siendo sus ataques más selectivos, con una mayor capacidad de planificación, por lo que podemos apreciar:

### A. Métodos.

Según estudio de Eleven Paths & Telefónica, (2016) los métodos de ciberextorsión son los siguientes (págs. 5-12):

**Figura 4**

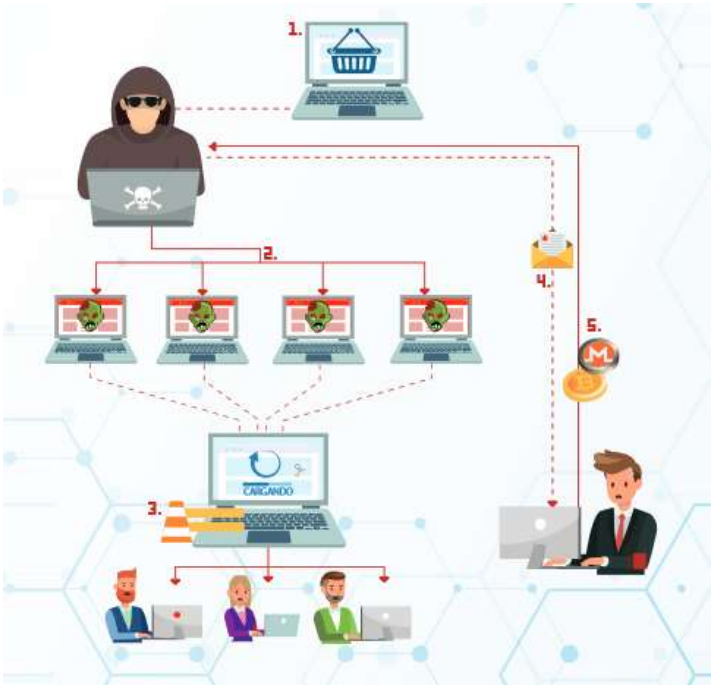
*Métodos de Ciberextorsiones*




Nota: En las ciberextorsiones, los ciberextorsionadores usan diferentes métodos. Adaptado de (Oficina de Seguridad del Internauta, 2018).

**Figura 5**

*Ataque de Denegación de Servicio*




Nota: Ilustración del método de Ataque de Denegación de Servicio que realiza el ciberextorsionador. Tomado de (CCIT, 2019).

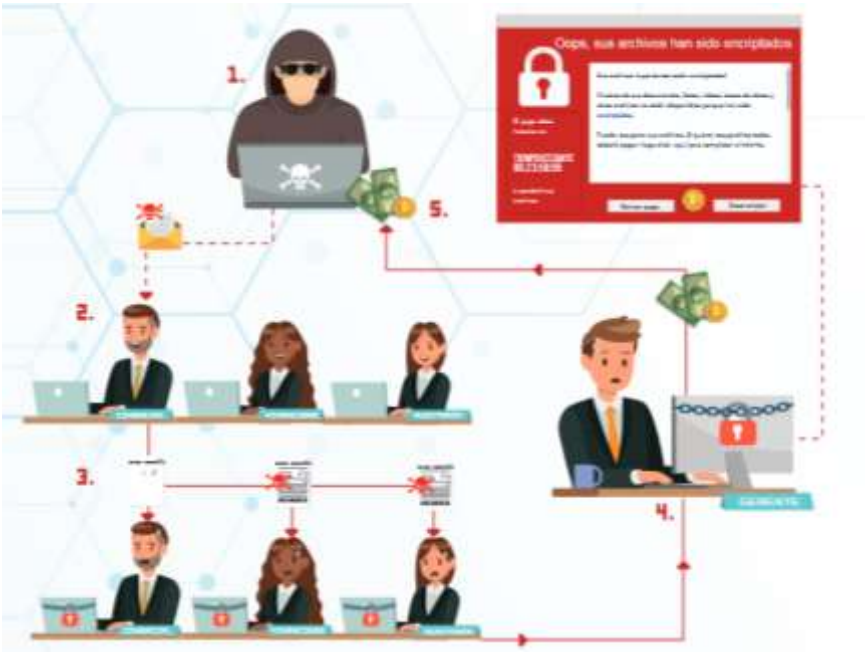
**Figura 6**

Robo de Información Confidencial

Nota: Ilustración del método de Robo de Información Confidencial que realiza el ciberextorsionador. Tomado de (Freepik, Sin Fecha).

**Figura 7**

*Malware Ransomware*




Nota: Ilustración del método de Malware Ransomware que realiza el ciberextorsionador. Tomado de (CCIT, 2019).

**B. Técnicas**

Entre las principales técnicas que utilizan los ciberextorsionadores tenemos:

**a. Ingeniería Social.**

Los Ciberextorsionadores usan mayormente las técnicas de Ingeniera Social para engañar a sus posibles cibervíctimas, para que estos instalen el malware. Esta es la forma más fácil, frecuente para el ciberextorsionador.

La manera en que lo realiza el ciberextorsionador es por correo, o por redes sociales, enviando un enlace de un mensaje suplantado de un amigo de la cibervíctima o una actualización supuesta de un software de uso común para enlazarlo e instalar el malware.

**b.Hunting**

Esta técnica los ciberextorsionadores buscan atacar y afectar a un gran número de cibervíctimas con una sola comunicación. Estás son el ransomware y el phishing.

**c.Farming**

Esta técnica los ciberextorsionadores realizan varias comunicaciones con las cibervíctimas con el fin de obtener mayor información.

### C. Herramientas

Los ciberextorsionadores utilizan miles de herramientas de acuerdo a su objetivo, son usados principalmente para el robo de información confidencial, vulnerabilidad de seguridad en software de sus cibervíctimas.

## 5. Modus Operandi de la Ciberextorsión

### A. Modus Operandi General

De manera general, la ciberextorsión se da de la siguiente manera:

**a. Selección de la Cibervíctima**

La cibervíctima es elegida por el ciberextorsionador quien hace uso de las redes sociales. En el caso de secuestro de datos en forma virtual, o bloqueo de sistemas, no se realiza la selección de la víctima porque se realiza de manera aleatoria.

**b. Disposición de la Información**

Etapa donde los ciberextorsionadores mediante correo electrónico, o Facebook comunican la información que poseen a su potencial víctima.

**c. Comunicación**

Etapa donde los ciberextorsionadores, se comunican a través de redes sociales como WhatsApp, Facebook, Instagram, o cuentas de correo para iniciar las conversaciones. Aquí se realizan las ciberamenaza.

**d. Exigencia Económica**

Etapa donde los ciberextorsionadores establecen un monto. En esta etapa también se realiza la negociación.

**e. Pago de la ciberextorsión**

La cibervíctima realiza el pago de la ciberextorsión. Si no se paga la ciberextorsión, el ciberextorsionador cumple su amenaza.

**Tabla 1**

*Modus Operandi de los ciberextorsionadores*

| Etapas | 1<br>Selección de la cibervíctima | 2<br>Disposición de la información | 3<br>Comunicación | 4<br>Exigencia Económica | 5<br>Pago de la ciberextorsión |
|---|---|---|---|---|---|
| Definición | Se escoge la cibervíctima potencial. No hay selección en secuestro de datos o bloqueo de sistemas. | Los ciberextorsionadores informan a la víctima la información que poseen. | Inician las conversaciones, se realiza la ciberamenaza | Se establece un monto, se realiza la negociación | La cibervíctima realiza el pago de la ciberextorsión, el ciberextorsio-nador logra su objetivo. |
| Obtención de Información | Web.<br>Base de datos. | Medios Informáticos. | Medios Informáticos. | Medios Informáticos. | Medios Informáticos. |
| medios que emplean | Medios Informáticos. | Correo electrónico.<br>Redes Sociales. | Correo electrónico.<br>Redes Sociales. | Correo electrónico.<br>Redes Sociales. | Transferencias bancarias.<br>Criptomonedas. |

Nota: El Modus Operandi en forma general que realizan los ciberextorsionadores. Elaboración propia.

Según el tipo de ciberamenazas, los ciberextorsionadores, realizan diferentes modus operandi. Así tenemos:

**B. Modus Operandi de Secuestro de Datos**

Los ciberextorsionadores, lanzan ataques a través de enlaces engañosos que pueden estar en e-mails, chats, o páginas web; lo hacen de la siguiente manera:

**Figura 8**

*Modus Operandi del Secuestro de Datos*


Nota: El modo operandi que usan los ciberextorsionadores en el secuestro de datos. Adaptado de (Statista, 2017) y (Macrovector, Hacker icon set with different types of hackers stealing information breaking computer system [Imagen], Sin fecha).

## C. Modus Operandi de Sextorsión

Las ciberextorsiones han evolucionado a través de los años, y para tener una idea más clara, a continuación, el modus operandi de la sextorsión o ciberextorsión sexual de antes, con lo de tiempos actuales:

**Figura 9**

*Modus Operandi Sextorsión*

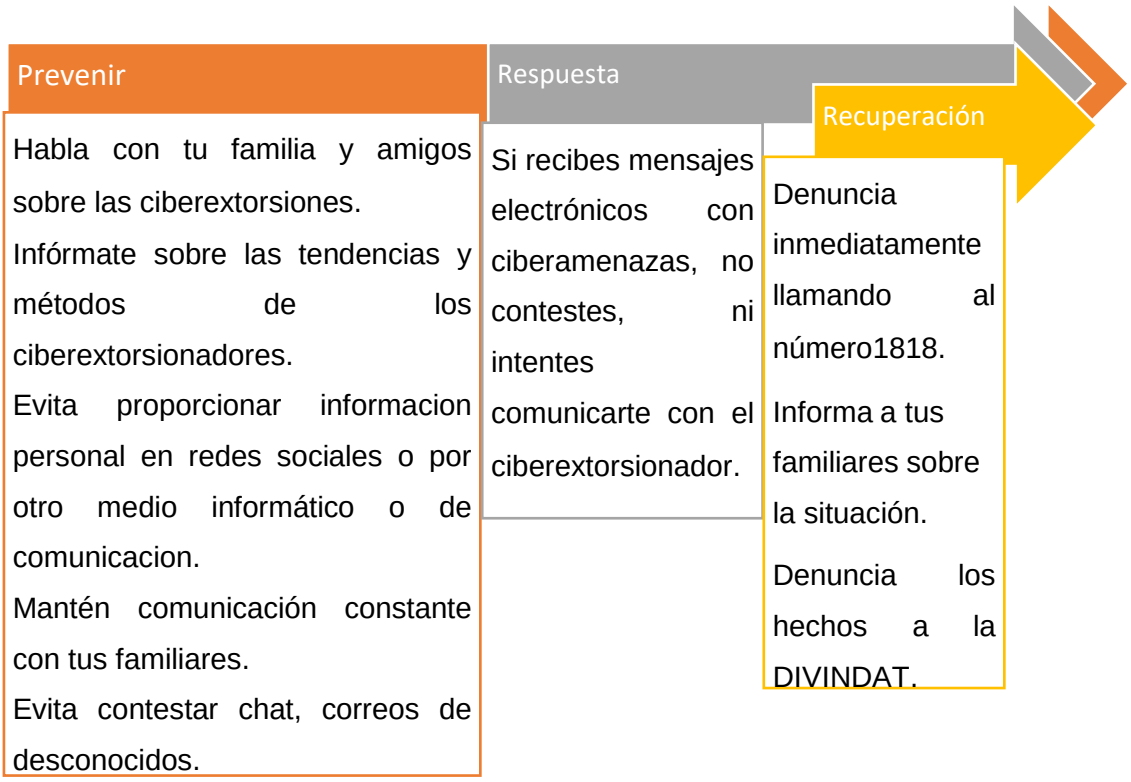

Nota: Modus Operandi que realizan los ciberextorsionadores en la sextorsión en comparación de antes con lo de ahora. Adaptado de (Trend Micro, 2015)

## 6. Medidas de seguridad para evitar la ciberextorsión

Entre las medidas de seguridad que podemos tener en cuenta para evitar la ciberextorsión tenemos:

**Figura 10**

*Medidas de Seguridad para evitar la ciberextorsión*




Nota: Medidas para la prevención y acción en caso de ciberextorsiones. Adaptado de: (Universidad de Guadalajara & SEMS, Sin Fecha).

Para la seguridad de los delitos de ciberextorsión, existe la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT – PNP de la DIRINCRI), creado para investigar, denunciar y combatir el crimen organizado cometidos mediante el uso de las tecnologías de información y telecomunicaciones (TIC's).

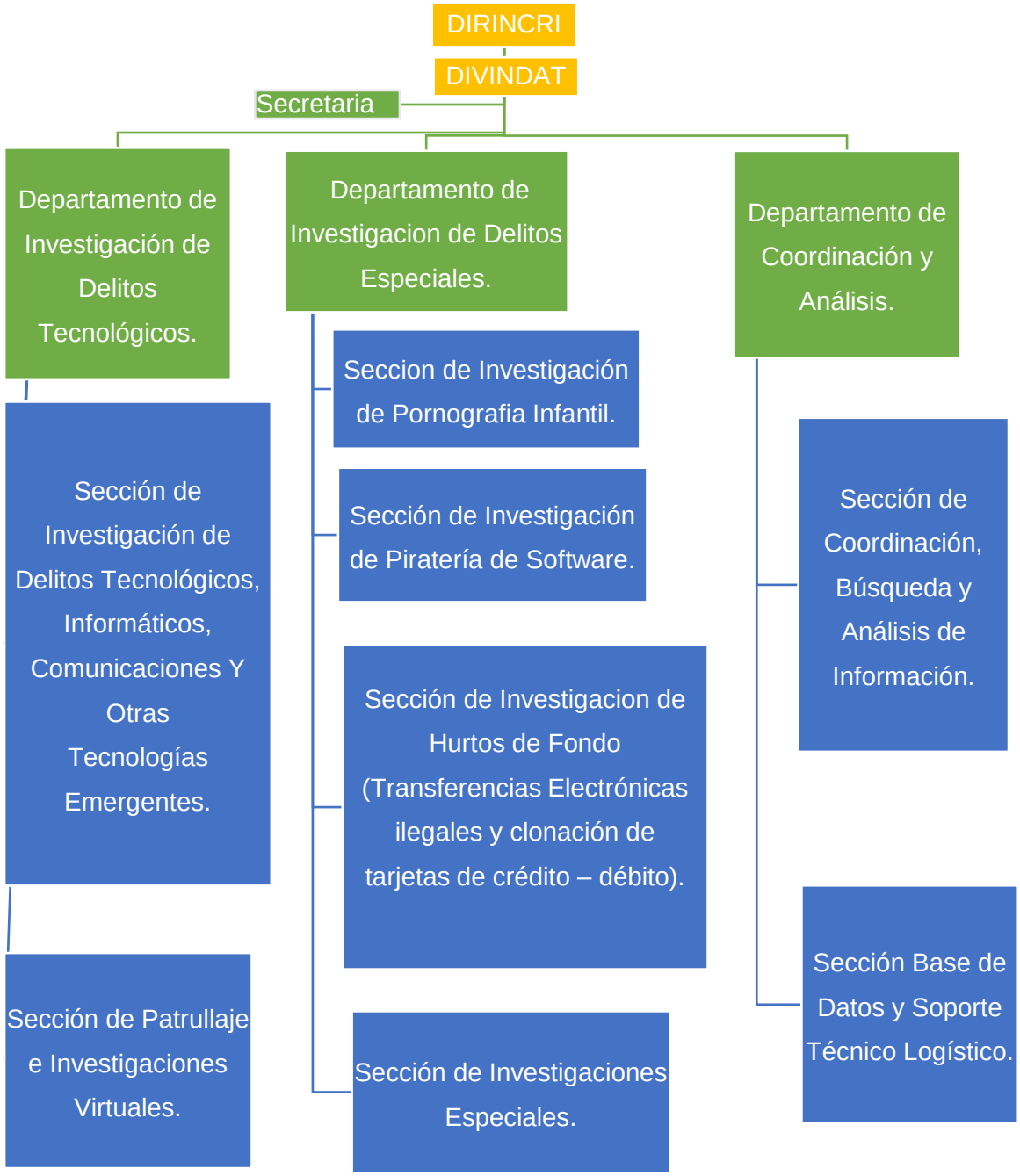
**Figura 11**

*Estrategias Operativas de la DIVINDAT*


Nota: La DIVINDAT realiza distintas acciones para combatir los delitos informáticos, entre ellas tenemos: acción preventiva, acción disuasiva, acción de búsqueda, acción investigadora, todas estas acciones lo realizan para combatir la ciberdelincuencia. Adaptado de (Chávez Retamozo, Sin Fecha).

**Figura 12**

*Estructura Orgánica de la DIVINDAT*




Nota: Organigrama con sus secciones de la DIVINDAT. Adaptado de (DIVINDAT, Organigrama DIVINDAT [Imagen], 2019).

## A. Herramientas de la DIVINDAT

La División de Investigación de delitos de Alta Tecnología - DIVINDAT, encargada de investigar, denunciar y combatir los delitos informáticos, realiza las siguientes actividades:

- Aprehende a los ciberdelincuentes.
- Identifica, ubica, detiene presuntos delitos, coactores y cómplices.
- Realiza patrullaje en redes sociales y otras.
- Recepciona e investiga denuncias de organismos internacionales (FBI, lnterpol, etc), y coordina acciones de inteligencia con entidades nacionales y extranjeras.

La División de Investigación de delitos de Alta Tecnología, se encuentra constantemente patrullando parte del ciberespacio, con la colaboración de la INTERPOL, EUROPOL, empresas de ciberseguridad, peritos forenses, plataformas digitales abogados digitales, que son aliados indispensables para revelar quién se está ocultando tras un correo electrónico, entre otros, esperan que los cibercriminales dejen evidencias digitales para que puedan ser detenidos y juzgados por sus delitos.

Actualmente la DIVINDAT cuenta con un cuerpo de efectivos constantemente capacitado en técnicas para extraer información de dispositivos electrónicos por medio de software, con lo cual obtienen evidencias digitales que les permite profundizar en las investigaciones, dar con los responsables de los hechos delictivos; adelantándose de esta manera a las organizaciones cibercriminales, en materia de tecnología para combatir con mejores herramientas los delitos informáticos que evolucionan, perfeccionan en todas sus modalidades en los dispositivos electrónicos.

La DIVINDAT se rige por leyes especiales, convenios, código de procedimiento, protocolos para actuar, combatir a los cibercriminales. En cuanto a su equipamiento es adecuado, que le permite obtener las evidencias

digitales para la reconstrucción de los hechos cibercriminales.

**Figura 13**

*Principales Ciberorganizaciones capturados por la DIVINDAT*

Caso: Organización Cibercriminal "Children Porn"

Red Cibercriminal de pedófilia de más de 170 integrantes, que a través de un grupo de Whatssapp promueven, distribuyen y publican imágenes, videos o enlaces virtuales con contenido de abuso infantil en varias provincias del Perú.

Caso: "Conexiones delitos contra el pudor"

Se efectuó el allanamineto de diez inmuebles en forma simultánea en el Callao, con la finalidad de desarticular una red criminal dedicada a la pornografía infantil, ofensas contra el pudor y delitos contra la libertad.

Caso " Los cibernéticos de Paruro"

Se intervino un establecimiento en el Cercado de Lima por comercializar codificadores de señales de satélite portadora de programas y otros, en agravio de las empresas América Móvil SAC, Telefónica del Perú, Direct TV Perú SRL.

Caso: Banda Internacionasl

"Teamkingn3t"

Una red internacional de hackers que opera en ocho países de América Latina, irrumpieron las págimas web de varias instituciones de Lima y provincias, la DIVINDAT identificó a quienes habían cometido estos delitos informáticos.

Caso: Los Elegantes de la Banca"

Se intervino banda delincuencial dedicada al delito informático contra el patrimonio, fraude informático agravado, atentado a la integridad de sistemas, mecanismos y dispositivos informáticos, en prejucio de conocidos bancos por un monto de S/. 558 000.00

Nota: Principales ciberorganizaciones capturadas por la DIVINDAT, en el año 2019. Adaptada de (DIVINDAT, División de Delitos de Alta Tecnología, 2019).

**B. Otras Instituciones del Estado Peruano para combatir la ciberextorsión**

Entre ellas tenemos a la Secretaría de Gobierno Digital, la Coordinadora de respuesta a emergencia en redes teleinformáticas de la administración pública del Perú (PECERT) y la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI).

**Tabla 2:**

*Otras Instituciones del Estado Peruano para combatir las ciberextorsiones*

| Sector | Institución | Acciones |
|---|---|---|
| Interior | División de Investigación de delitos de alta tecnología (DIVINDAT). | Investigación de delitos cibernéticos. |
| Ministerio Público. | Fiscalías penales y mixtas. | Investigación de delitos cibernéticos. |
| Poder Judicial. | Juzgados penales y mixtos. | Sanción a casos de delitos cibernéticos. |
| Presidencia del Consejo de Ministros. | Secretaría de Gobierno Digital. | Lidera los procesos de innovación tecnológica y de transformación digital del Estado. Es el ente rector del Sistema Nacional de Transformación Digital y administra las Plataformas Digitales del Estado peruano. |

| Sector | Institución | Acciones |
|---|---|---|
| Presidencia del Consejo de Ministros | Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) | Encargado de dirigir como ente rector, el Sistema Nacional de Informática y de implementar la Política Nacional de Gobierno Electrónico e Informática. |
| Presidencia del Consejo de Ministros | Coordinadora de respuesta a emergencia en redes teleinformáticas de la administración pública del Perú (PECERT) - Presidencia del Consejo de Ministros | Encargado de liderar los esfuerzos para resolver, anticipar y enfrentar los Ciberdesafíos y coordinar la defensa ante los Ciberataques, con el fin de proveer a la Nación de una postura Segura en el Ámbito de la Seguridad Digital. |

Nota: Instituciones peruanas que combaten las ciberextorsiones. Adaptada de (Consejo Nacional de Política Criminal CONAPOC, 2020, pág. 56).

## 7. Normatividad del Delito de Ciberextorsión

### A. Código Penal Peruano

El artículo 200ª sobre extorsión establece que:

> 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 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 ciberextorsión, 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, 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.(Ministerio de Justicia & Sistema Peruano de Información Jurídica, 2018, págs. 202-203).

El capítulo X, sobre Delitos Informáticos, en sus artículos 207-A, 207-B, 207-C y 207-D, fue derogado por la “Única Disposición Complementaria Derogatoria de la Ley N.º 30096, publicada el22 octubre 2013”.(Ministerio de Justicia & Sistema Peruano de Información Jurídica, 2018, págs. 210-211).

**B. La Ley N° 30096 - Ley de Delitos Informáticos**

La presente Ley tiene por objeto prevenir, sancionar las conductas ilícitas que afectan los sistemas, datos informáticos, 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. **(Congreso de la República, 2013, pág. 1)**.

La Ciberextorsión forma parte de los delitos informáticos, en el Perú se ha suscrito al Convenio de Budapest, el primer tratado que establece herramientas de derecho penal y acuerdos de cooperación judicial internacional para combatir el cibercrimen.

C. **Convenido de Budapest**

El Convenio de Budapest fue adoptado en fecha 23 de noviembre de 2001, se creó para "aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional; aplicar una política penal común para proteger a la sociedad de la ciberdelincuencia, enfrentando los delitos informáticos".**(Ministerio de Relaciones Exteriores, 2019, pág. 2)**.

El Perú se adhirió al Convenio de Budapest el 12 de febrero de 2019, mediante Resolución Legislativa Nº 30913, ratificada a través del Decreto Supremo Nº 010-2019-RE el 9 de marzo de 2019. El convenio de Budapest entró en vigencia el 1º de diciembre de 2019 en Perú.

El Convenio Budapest, en materia penal, propone medidas sobre la sobre Ciberdelincuencia la recolección, interceptación, disposición, conservación de datos informáticos; estas medidas ya han sido adoptadas por las modificaciones de la Ley 30096, y el artículo 230 del Nuevo Código Procesal Penal, pero existen otras medidas que el Perú todavía no adoptado.

Los países miembros de América Latina y el Caribe que ya forman parte del convenio de Budapest, son: República Dominicana desde el año 2013, Panamá desde el año 2014, Costa Rica desde el año 2017, Chile desde el año 2017, Argentina desde el año 2018, Paraguay desde el año 2018, Perú desde el año 2019; Colombia desde el año 2020; mientras que los países México, Guatemala, Brasil están invitados a participar ascender y ser parte del convenio de Budapest.

**Figura 14**

*Lista de Países adheridos a la convención de Budapest*


Nota: Países miembros y países invitados a la convención de Budapest. Tomado de (Ciberseguridad, OEA, & BID, 2020).

**D. Ley de ciberdefensa – Ley 30999**

La ley de ciberdefensa en el Perú, fue promulgada el 9 de agosto de 2019, con el objetivo de "establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley" **(Ley Nº 30999 - Ley de Ciberdefensa, 2019, pág. 9)**.

Esta ley ejecuta operaciones a los militares de ciberdefensa en el ciberespacio, con el fin que actúen frente a las ciberamenazas, o los ciberataques que afecten la seguridad nacional.

E. **Política Nacional de Ciberseguridad**

Las Políticas Nacional de Ciberseguridad, tiene como finalidad elaborar un Plan de Acción Nacional en temas de Seguridad, en forma multidisciplinaria y multisectorial. Así mismo establece la creación nacional de Ciberseguridad.

Entre sus objetivos tenemos:

- Proteger la infraestructura de información, los datos e información del Estado y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Asegurar la implementación de las propuestas legislativas, y en general la normatividad relacionada con la seguridad de la información, o ciberseguridad comprendida en esta Política, identificando los recursos involucrados y las partidas presupuestales correspondientes.
- Mantener la Política Nacional de Ciberseguridad actualizada, a efectos de asegurar su vigencia y por ende su eficacia,

promoviendo la participación de las entidades de sector público y privado, así como representantes de la sociedad civil y la academia. (Presidencia del Consejo de Ministros, Congreso de la República, pág. 1),

## 8. La ciberextorsión en la Ley Nº 30096 de Delitos Informáticos

### A. Términos específicos de la Ley Nº 30096 sobre ciberextorsión

Dentro de la ley Nº 30096, en Disposiciones Complementarias y Modificatorias, en su artículo Nº 1: Marco y Finalidad, solo menciona la ciberextorsión, como un delito, en donde los jueces pueden hacer uso de la ley Nº 30096.

De manera más específica y reglamentaria, la ciberextorsión no se encuentra tipificada de manera expresa, para su adecuado tratamiento, ya que es de suma importancia en estos tiempos actuales, en donde las ciberextorsiones están en aumento.

Es necesario que como avanza las nuevas modalidades de ciberextorsiones, la ley debe adecuarse, actualizarse e incluir de manera expresa los delitos de ciberextorsión y otros delitos informáticos que no están regulados de manera expresa.

De esta manera se establecerá reglas para la ciberextorsión, se mejorará la seguridad nacional, para el bienestar de la ciudadanía; a la vez se estaría cumpliendo con adecuar la legislación peruana, con lo acordado en el convenio de Budapest.

## 9. Las ciberextorsiones en el Perú

### A. Delitos Informáticos en la DIVINAT a nivel nacional

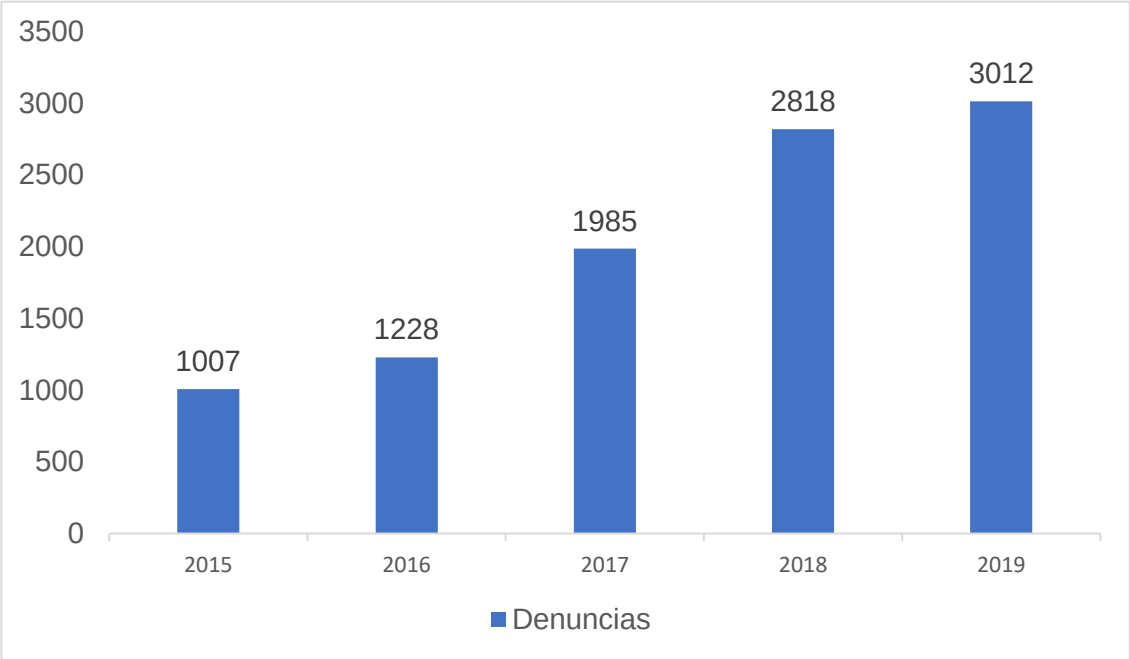
En el Perú, las ciberextorsiones como otros delitos informáticos se mantienen en constante innovación, crecimiento; con la existencia de la pandemia, las

cifras son considerables.

“Las cifras de denuncias por delitos cibernéticos vienen aumentando cada año. En cinco años se han atendido 10 110 denuncias correspondientes a delitos informáticos; en un notorio ascenso que alcanza a triplicarse de forma sostenida en el tiempo”(Consejo Nacional de Política Criminal CONAPOC, 2020, pág. 37).

**Figura 15:**

*Números de denuncias de Delitos Informáticos registrados en la DIVINDAT a nivel nacional 2015-2019*



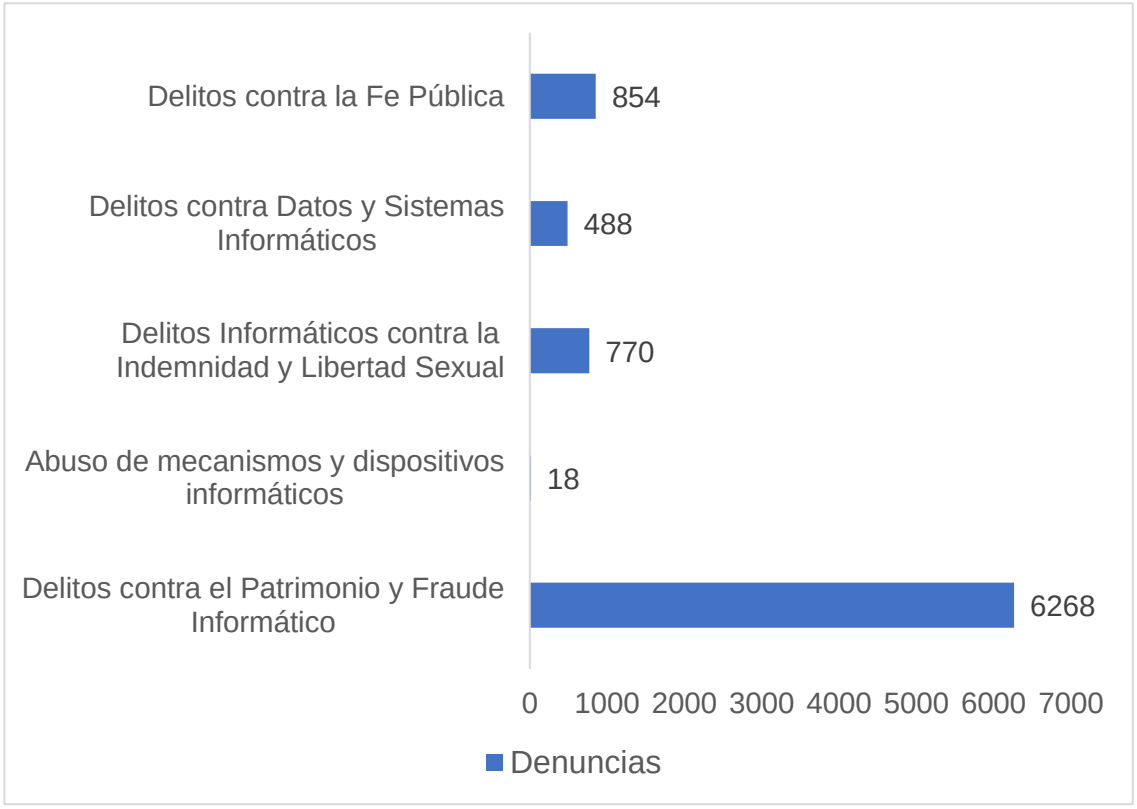

Nota: Denuncias de delitos informáticos entre los años 2015 al 2019 realizados en la DIVINDAT. Adaptado de (Consejo Nacional de Política Criminal CONAPOC, 2020).

De manera desagregada, según el tipo de ciberdelitos, durante los 5 años (2015 -2019), los delitos que más prevalecen son los delitos Informáticos contra el patrimonio y fraude informático, que se registraron 6,268 denuncias de delitos en la DIVINDANT.

El método más usado que se ha empleado durante los 5 años, es el phishing, en donde los ciberdelincuentes se hacen pasar por grandes entidades financieras bancarias, organizaciones no gubernamentales, empresas de alto nivel de prestigio; recurren a diversas herramientas como e-mails, llamadas telefónicas, mensajes de WhatsApp, páginas fraudulentas y engañosas, redes sociales como Facebook, Twitter, Instagram, Snapchat; para pescar los datos que son sus posibles cibervíctimas para realizar sus actividades ciberdelictivas, cometer el ciberdelito y obtener cantidades de dinero.

**Figura 16:**

*Número de denuncias, según Delitos Informáticos registrados en la DIVINDAT a nivel nacional 2015-2019*




Nota: Las denuncias mayores registradas en la DIVINDANT son de Delitos contra el Patrimonio y Fraude Informático. Adaptado de (Consejo Nacional de Política Criminal CONAPOC, 2020).

Según La División de Investigación de Delitos de Alta Tecnología (DIVINDAT), en el año 2019 se registró 3,012 denuncias de Delitos Informáticos, cifra mayor con respecto a los demás delitos, entre los que destacan los fraudes informáticos; sus subtipos, alcanzando 2,097 denuncias durante el 2019. Esta cifra aumento en 8% con respecto al año 2018, que cerró con 1,928 casos.

Del total de denuncias, 1,641 denuncias se registraron sobre transacciones no autorizadas vía internet. También hubo 431 casos de compras fraudulentas y 25, de clonación de tarjetas de crédito o débito.

El acoso sexual, las estafas en línea, amenazas desde mensajería o redes sociales o la extorsión, en donde los emplearon herramientas digitales como redes sociales, software y otras plataformas en línea se registran 268 denuncias en el año 2019, mientras que en el año 2018 hubo 362 denuncias.

Se registraron 247 casos de suplantación de identidad en el 2019. Las proposiciones a niños, niñas y adolescentes con fines sexuales desde mecanismos digitales o las denuncias de pornografía infantil sumaron 237 en el 2019.

El acceso ilícito, el tráfico ilegal de datos, los atentados a la integridad de sistemas informáticos o de datos alcanzaron 161 denuncias durante el año 2019. (Pichihua, Andina- Agencia Peruana de Noticias, 2020).

“De enero a junio del 2020, se ha registrado 1,476 denuncias de Delitos Informáticos, registrando mayores casos en fraudes informáticos, con 929 casos”. (Pichihua, Andina -Agencia Peruana de Noticias, 2020).

**Tabla 3**

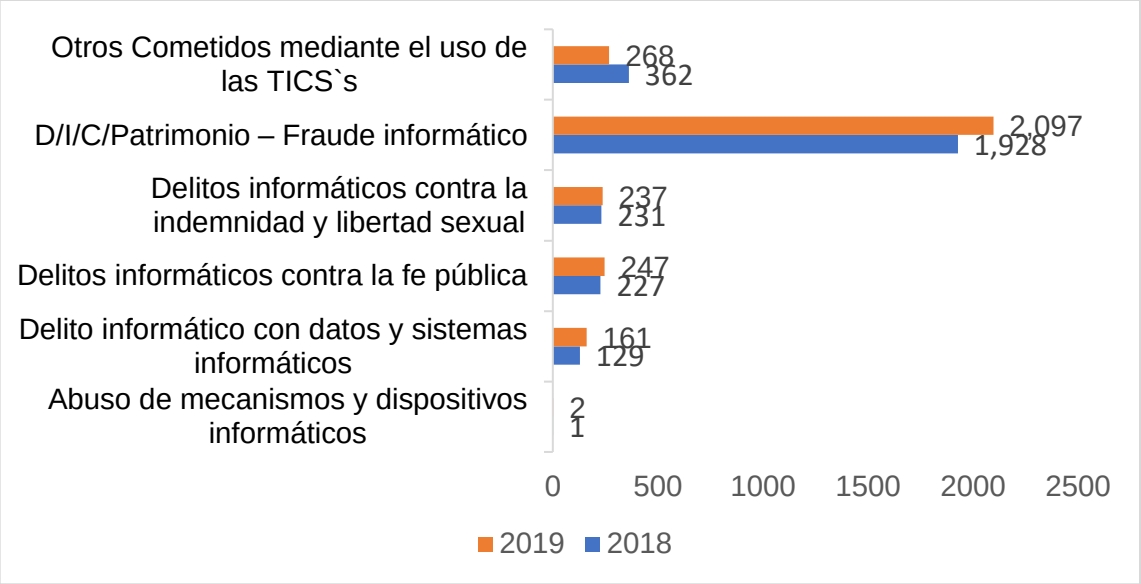
*Delitos Informáticos de denuncias en la DIVINDAR a nivel nacional 2018-2019*

| Por tipo de Delito Informático | 2018 | 2019 |
|---|---|---|
| Abuso de mecanismos y dispositivos informáticos | 1 | 2 |
| Delito informático con datos y sistemas informáticos | 129 | 161 |
| Delitos informáticos contra la fe pública | 227 | 247 |
| Delitos informáticos contra la indemnidad y libertad sexual | 231 | 237 |
| D/I/C/Patrimonio – Fraude informático | 1,928 | 2,097 |
| Otros Cometidos mediante el uso de las TICS`s | 362 | 268 |
| Total | 2,878 | 3,012 |

Nota: Denuncias de ciberdelitos en la DIVINDAT, durante los años 2018-2019. Adaptado de (Pichihua, Andina- Agencia Peruana de Noticias, 2020).

**Figura 17**

*Delitos Informáticos de denuncias registradas en la DIVINDAT a nivel nacional 2018-2019*




Nota: Denuncias de ciberdelitos en la DIVINDAT, durante los años 2018-2019, con más cifras de denuncias Delito Informático contra el Patrimonio y Fraude Informático. Adaptado de (Pichihua, Andina- Agencia Peruana de Noticias, 2020).

**Tabla 4**

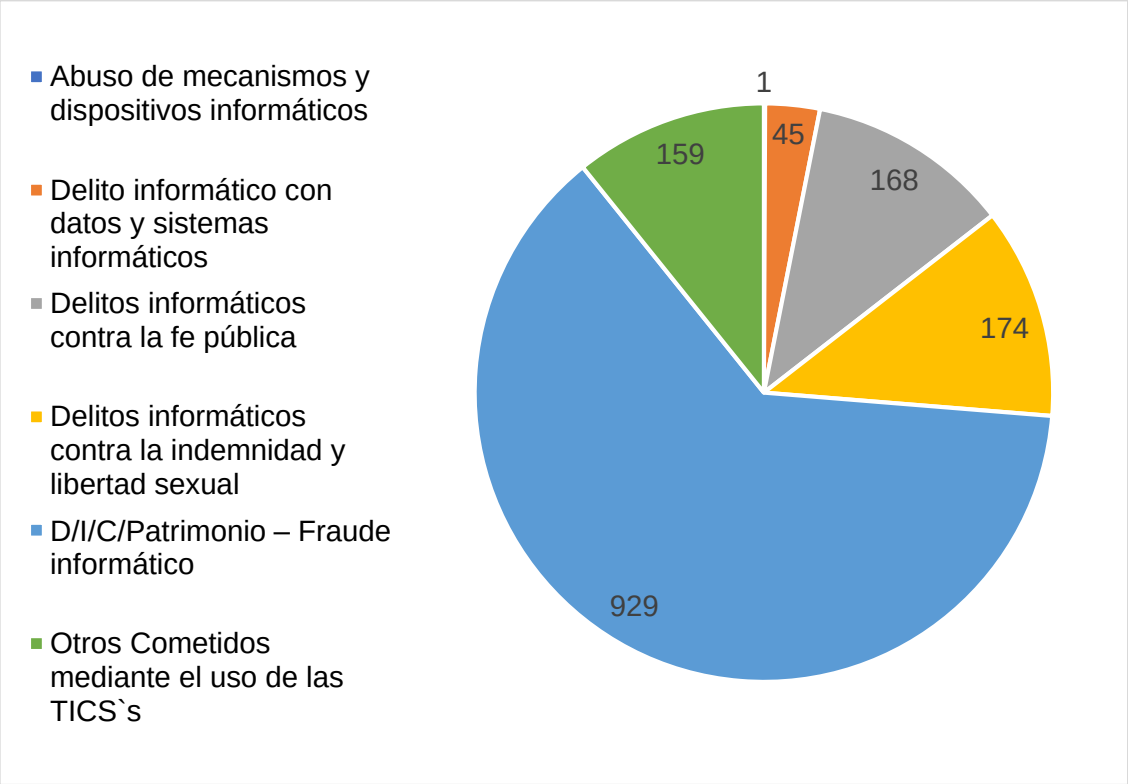
*Denuncias de ciberdelitos en enero a junio 2020 en la DIVINDAT*

| Por tipo de Delito Informático | 2020 enero - junio |
|---|---|
| Abuso de mecanismos y dispositivos informáticos | 1 |
| Delito informático con datos y sistemas informáticos | 45 |
| Delitos informáticos contra la fe pública | 168 |
| Delitos informáticos contra la indemnidad y libertad sexual | 174 |
| D/I/C/Patrimonio – Fraude informático | 929 |
| Otros Cometidos mediante el uso de las TICS`s | 159 |
| Total | 1,476 |

Nota: Las denuncias mayores son de ciberdelitos contra el Patrimonio y Fraude Informático. Adaptado de(Pichihua, Andina -Agencia Peruana de Noticias, 2020).

**Figura 18**

*Denuncias registradas en la DIVINDAT de enero a junio 2020 de ciberdelitos*




Nota: Los ciberdelitos con mayor denuncia son contra el Patrimonio y Fraude Informático. Adaptado de (Pichihua, Andina -Agencia Peruana de Noticias, 2020).

**B. Delitos en Fiscalía a nivel nacional**

En el año 2016, desde enero a diciembre se registraron 610,182 delitos, siendo 937 delitos que corresponde a Delitos Informáticos, representado en 0.15% de delitos registrados.

"Durante el período enero – diciembre del 2017 se registraron en el Ministerio Público 740,047 delitos penales de los cuales son delitos informáticos de la ley N°30096: 2,530 delitos representando el 0.34% de delitos registrados".(Ministerio Público - Fiscalía de la Nación, Boletín Estadístico del Ministerio Público Diciembre 2017, 2018, pág. 59).

"Al mes de diciembre del 2018, se registraron en el Ministerio Público 909,750

delitos penales de los cuales son delitos informáticos Ley N°30096: 4,304 delitos, representando el 0.47% de delitos registrados".(Ministerio Público - Fiscalía de la Nación, Boletín Estadístico Diciembre 2018, 2019, pág. 44).

**Tabla 5**

*Delitos Genéricos de denuncias registradas en Fiscalías Provinciales Penales y Mixtas a nivel nacional 2016-2018*

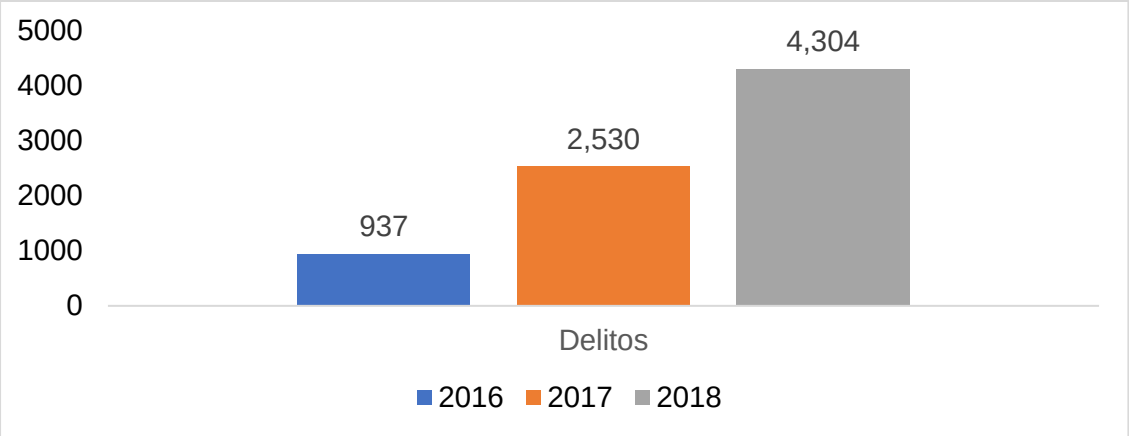
| Delitos Genéricos | 2016 | | 2017 | | 2018 | |
|---|---|---|---|---|---|---|
| | Nº Delitos | % | Nº Delitos | % | Nº Delitos | % |
| Contra la Vida, el Cuerpo y la Salud | 151,619 | 24.85 | 229,698 | 31.04 | 322,776 | 35.49 |
| Contra el Patrimonio | 197,059 | 32.30 | 223,940 | 30.26 | 282,275 | 31.03 |
| Contra la Seguridad Pública | 71,604 | 11.73 | 87,053 | 11.76 | 81,331 | 8.94 |
| Contra la Administración Publica | 46,087 | 7.55 | 48,613 | 6.57 | 52,262 | 5.74 |
| Contra la Libertad | 42,942 | 7.04 | 44,347 | 5.99 | 49,896 | 5.48 |
| Contra la Familia | 56,101 | 9.19 | 60,103 | 8.12 | 69,491 | 7.64 |
| Contra la Fe Pública | 21,952 | 3.60 | 22,618 | 3.06 | 24,593 | 2.70 |
| Delitos Ambientales | 5,616 | 0.92 | 5,717 | 0.77 | 6,956 | 0.76 |
| Ley Nº 30096, Ley de Delitos Informáticos | 937 | 0.15 | 2,530 | 0.34 | 4,304 | 0.47 |
| Contra la Tranquilidad Pública | 3,827 | 0.63 | 3,821 | 0.52 | 3,236 | 0.36 |
| Otros Delitos Genéricos (*) | 12,438 | 2.04 | 11,607 | 1.57 | 12,630 | 1.39 |
| Total | 610,182 | 100 | 740,047 | 100 | 909,750 | 100 |

Nota: Las denuncias registradas entre los años 2016 al 2018 han ido en aumento. Adaptado de:

(Ministerio Público - Fiscalía de la Nación, Boletín Estadístico Diciembre 2018, 2019) y (Ministerio Público - Fiscalía de la Nación, Boletín Estadístico del Ministerio Público Diciembre 2017, 2018).

**Figura 19:**

*Delitos Informáticos de denuncias registrados en las Fiscalías Provinciales Penales y Mixtas a nivel nacional 2016-2018*




Nota: Las denuncias registradas de ciberdelitos en el año 2016 es mucho menor que el año 2017 y 2018. (Ministerio Público - Fiscalía de la Nación, Boletín Estadístico Diciembre 2018, 2019) y (Ministerio Público - Fiscalía de la Nación, Boletín Estadístico del Ministerio Público Diciembre 2017, 2018).

En el periodo de enero a julio del 2017, se registraron 412,628 denuncias de delitos penales en el Ministerio Público, de los cuales 1,357 son denuncias registradas de Delitos Informáticos, representando el 0.33% de Delitos Genéricos totales.

"Al mes de julio del 2018, se registraron 487,933 delitos penales de los cuales son delitos informáticos leyN°30096: 2,085 delitos, representando el 0.43% de delitos registrados"(Ministerio Público - Fiscalía de la Nación, Boletín Estadístico Julio 2018, 2018, pág. 44).

En los meses de enero a julio del 2019, se registraron 616,437 delitos penales, de los cuales 3,908 corresponde a delitos Informáticos, representando el 0.63% de delitos totales.

“El Ministerio Público registró 299, 852 delitos Penales, en el periodo de enero a junio 2020; de los cuales el 0.88% representa los delitos informáticos.”(Ministerio Público - Fiscalía de la Nación, Boletín Estadístico del Ministerio Público Julio 2020, 2020, pág. 40).

“Durante los meses de enero a diciembre del 2017 se registró un total de 2,530 delitos informáticos, cifra mayor en un 170.01% a los delitos registrados en el mismo período del año 2016 que fueron de 937 delitos” (Ministerio Público - Fiscalía de la Nación, Boletín Estadístico del Ministerio Público Diciembre 2017, 2018, pág. 69).

“Al mes de diciembre del año 2018, se registró un total de 4,304 delitos informáticos, cifra mayor en un 70.12% a los delitos registrados en el mismo período del año 2017 que fueron de 2,530 delitos”(Ministerio Público - Fiscalía de la Nación, Boletín Estadístico Diciembre 2018, 2019, pág. 54).

“Durante el año 2019, el Ministerio Público ha atendido un total de 4636 casos de ciberdelitos; siendo los casos de daño al patrimonio y fraude informático, los más significativos, con un total de 1788 incidentes”.(Consejo Nacional de Política Criminal CONAPOC, 2020, pág. 38).

“Al mes de julio del año 2018, se registró un total de 2,085 delitos informáticos, cifra mayor en un 53.65% a los delitos registrados en el mismo período del año 2017 que fueron de 1,357 delitos” (Ministerio Público - Fiscalía de la Nación, Boletín Estadístico Julio 2018, 2018, pág. 54).

“El Ministerio Público registró de 2,644 delitos informáticos, en el periodo de enero a junio 2020; cifra menor en un 32.34% a los delitos registrados en el mismo período del año 2019 que fueron de 3,908 delitos.”(Ministerio Público - Fiscalía de la Nación, Boletín Estadístico del Ministerio Público Julio 2020, 2020, pág. 48).

**Tabla 6**

*Delitos Genéricos de denuncias registradas en Fiscalías Provinciales y Mixtas a nivel nacional en enero a julio 2017-2020*

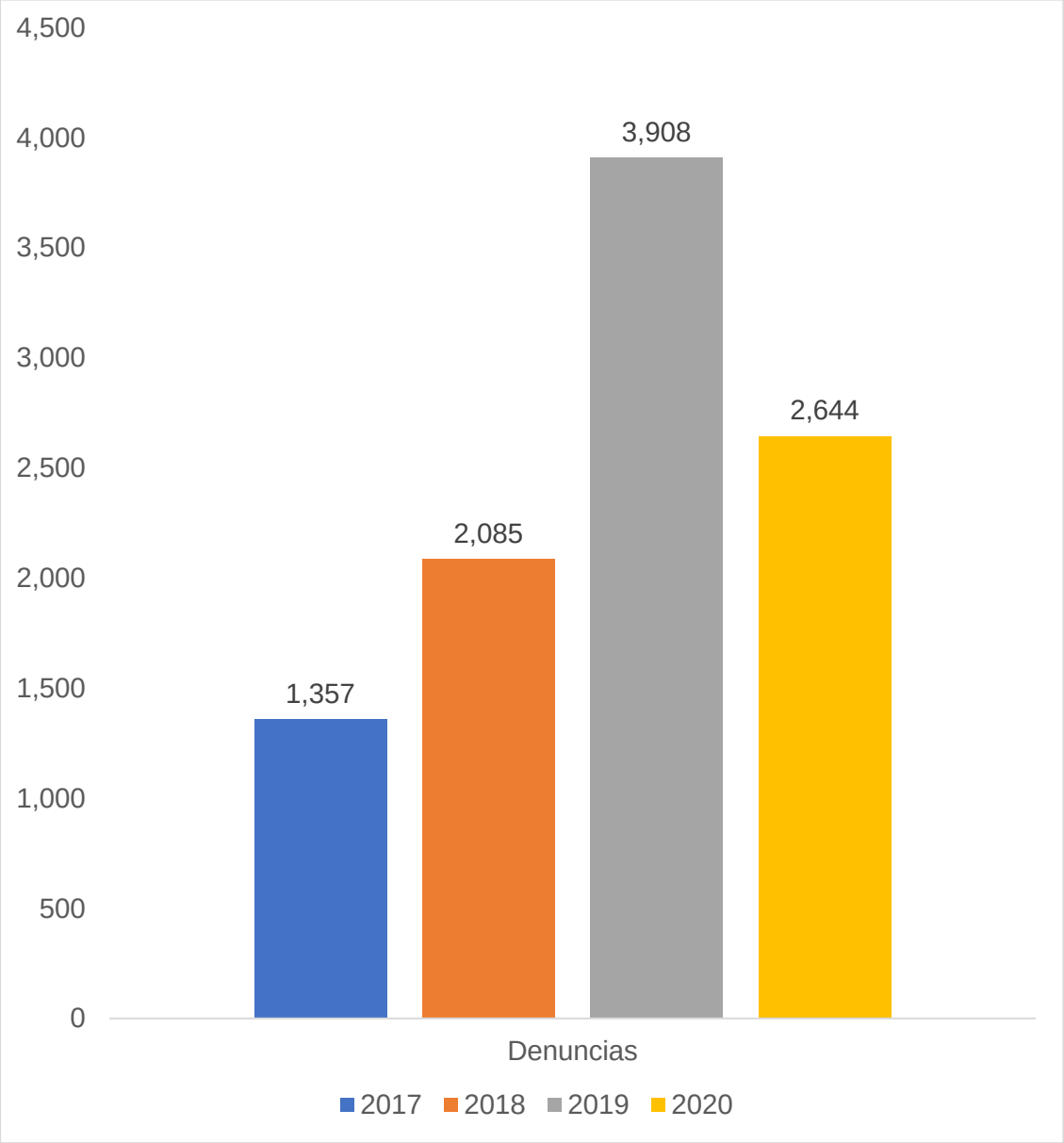
| Delitos Genéricos | 2017 Enero-Julio | | 2018 Enero-Julio | | 2019 Enero-Julio | | 2020 Enero-Julio | | |
|---|---|---|---|---|---|---|---|---|---|
| | Nº Delitos | % | Nº Delitos | % | Nº Delitos | % | Nº Delitos | % | % Variación |
| Contra la Vida, el Cuerpo y la Salud | 124,204 | 30.10 | 169,895 | 34.81 | 240,055 | 38.94 | 122,915 | 41.00 | -48.80 |
| Contra el Patrimonio | 125,197 | 30.34 | 148,299 | 30.39 | 186,961 | 30.33 | 82,396 | 27.48 | -55.93 |
| Contra la Seguridad Pública | 50,005 | 12.12 | 50,096 | 10.27 | 46,186 | 7.49 | 25,831 | 8.61 | -44.07 |
| Contra la Administración Publica | 28,623 | 6.94 | 28,151 | 5.77 | 35,602 | 5.78 | 20,887 | 6.97 | -41.33 |
| Contra la Libertad | 25,433 | 6.16 | 26,768 | 5.49 | 33,505 | 5.44 | 17,693 | 5.90 | -47.19 |
| Contra la Familia | 33,341 | 8.08 | 36,830 | 7.55 | 42,791 | 6.94 | 13,885 | 4.63 | -67.55 |
| Contra la Fe Pública | 12,471 | 3.02 | 13,589 | 2.79 | 13,488 | 2.19 | 5,900 | 1.97 | -56.26 |
| Delitos Ambientales | 3,088 | 0.75 | 3,877 | 0.79 | 4,552 | 0.74 | 2,846 | 0.95 | -37.48 |

| Delitos Genéricos | 2017 Enero-Julio | | 2018 Enero-Julio | | 2019 Enero-Julio | | 2020 Enero-Julio | | |
|---|---|---|---|---|---|---|---|---|---|
| | Nº Delitos | % | Nº Delitos | % | Nº Delitos | % | Nº Delitos | % | Variación |
| Ley Nº 30096, Ley de Delitos Informáticos | 1,357 | 0.33 | 2,085 | 0.43 | 3,908 | 0.63 | 2,644 | 0.88 | -32.34 |
| Contra la Tranquilidad Pública | 2,273 | 0.55 | 1,907 | 0.39 | 1,930 | 0.31 | 883 | 0.29 | -54.25 |
| Otros Delitos Genéricos (*) | 6,636 | 1.61 | 6,436 | 1.32 | 7,459 | 1.21 | 3,972 | 1.32 | -46.75 |
| Total | 412,628 | 100.00 | 487,933 | 100.00 | 616,437 | 100.00 | 299,852 | 100.00 | -51.36 |

Nota: En el periodo de enero a julio de 2020, se muestra una pequeña disminución de denuncias de ciberdelitos registradas en las Fiscalías con respecto al periodo de enero a julio de 2019. Adaptado de (Ministerio Público - Fiscalía de la Nación, Boletín Estadístico Julio 2018, 2018, pág. 44) y (Ministerio Público - Fiscalía de la Nación, Boletín Estadístico del Ministerio Público Julio 2020, 2020, pág. 40).

**Figura 20**

*Delitos Informáticos registrados en Fiscalías Penales y Mixtas a nivel nacional en enero a junio 2017-2020*




Nota: En el periodo de enero a julio de 2020, se muestra una pequeña disminución de denuncias de ciberdelitos registras en las Fiscalías con respecto al periodo de enero a julio de 2019. Adaptado de (Ministerio Público - Fiscalía de la Nación, Boletín Estadístico Julio 2018, 2018, pág. 44) y (Ministerio Público - Fiscalía de la Nación, Boletín Estadístico del Ministerio Público Julio 2020, 2020, pág. 40).

**Tabla 7**

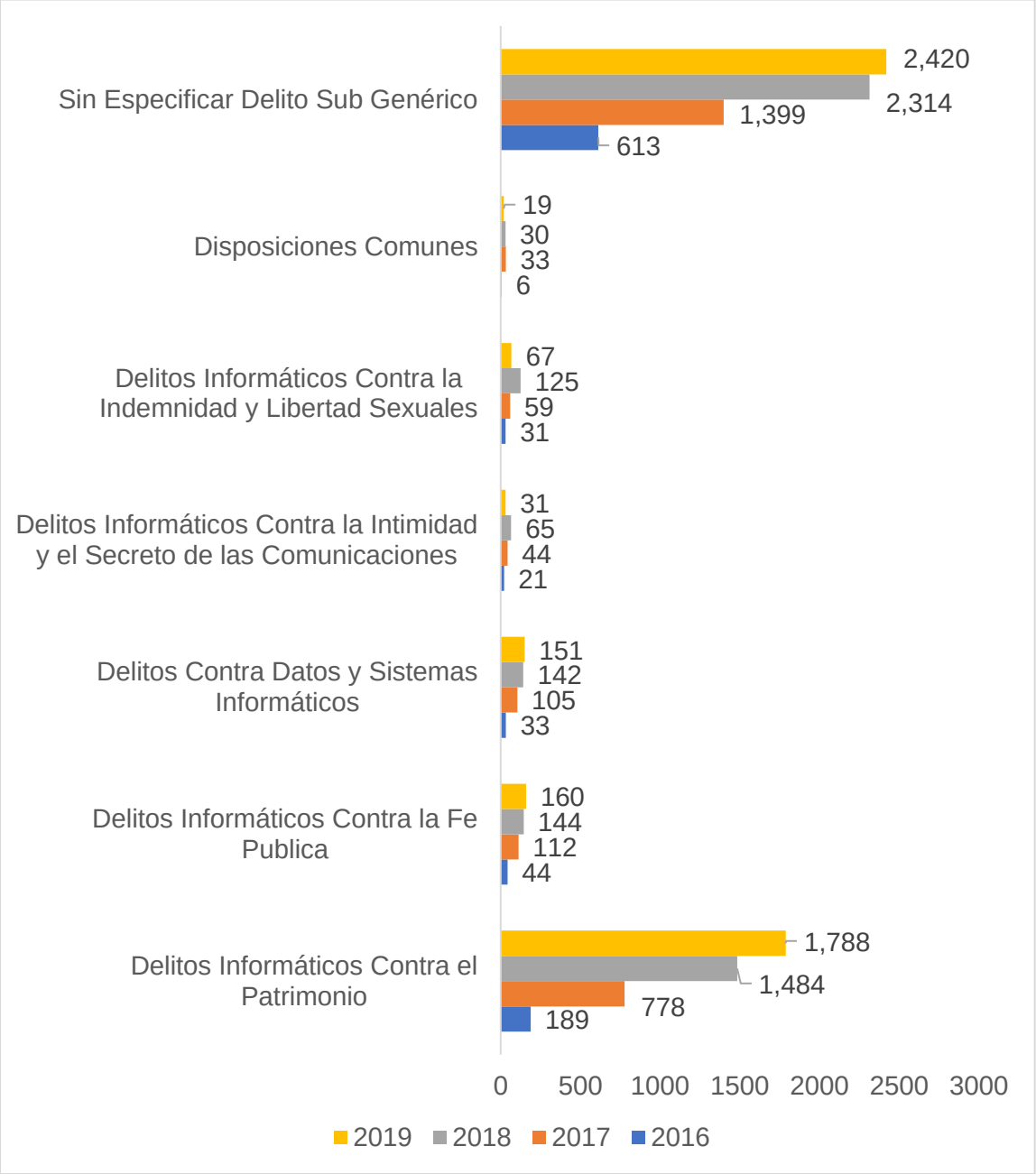
*Delitos Informáticos de denuncias registradas en Fiscalías Provinciales Penales y Mixtas a nivel nacional 2016 -2019*

| Delitos Sub Genéricos | 2016 | | 2017 | | 2018 | | 2019 | |
|---|---|---|---|---|---|---|---|---|
| | Nº Delitos | % | Nº Delitos | % | Nº Delitos | % | Nº Delitos | % |
| Ley Nº 30096, Ley de Delitos Informáticos | | | | | | | | |
| Delitos Informáticos Contra el Patrimonio | 189 | 20.17 | 778 | 30.75 | 1,484 | 34.48 | 1,788 | 38.60 |
| Delitos Informáticos Contra la Fe Publica | 44 | 4.70 | 112 | 4.43 | 144 | 3.35 | 160 | 3.50 |
| Delitos Contra Datos y Sistemas Informáticos | 33 | 3.52 | 105 | 4.15 | 142 | 3.30 | 151 | 3.30 |
| Delitos Informáticos Contra la Intimidad y el Secreto de las Comunicaciones | 21 | 2.24 | 44 | 1.74 | 65 | 1.51 | 31 | 0.70 |
| D/I/C/ la Indemnidad y LibertadSexuales | 31 | 3.31 | 59 | 2.33 | 125 | 2.90 | 67 | 1.40 |
| Disposiciones Comunes | 6 | 0.64 | 33 | 1.30 | 30 | 0.70 | 19 | 0.40 |
| Sin Especificar Delito Sub Genérico | 613 | 65.42 | 1,399 | 55.30 | 2,314 | 53.76 | 2,420 | 52.2 |
| Total | 937 | 100 | 2,530 | 100 | 4,304 | 100 | 4,636 | 100 |

Nota: Durante los años 2016 al 2019, los ciberdelitos han aumentado. Adaptado de: (Ministerio Público - Fiscalía de la Nación, Boletín Estadístico del Ministerio Público Diciembre 2017, 2018, pág. 69) y(Consejo Nacional de Política Criminal CONAPOC, 2020, pág. 38).

**Figura 21**

*Delitos Informáticos registrados en Fiscalías Penales y Mixtas a nivel nacional 2016-2019*




Nota: El incremento de los ciberdelitos ha ido en aumento en los años 2016 a 2019.Adaptado de: (Ministerio Público - Fiscalía de la Nación, Boletín Estadístico del Ministerio Público Diciembre 2017, 2018, pág. 69) y(Consejo Nacional de Política Criminal CONAPOC, 2020, pág. 38).

**Tabla 8**

*Delitos Informáticos de denuncias registradas en Fiscalías Provinciales Penales y Mixtas. Enero a julio 2017-2020*

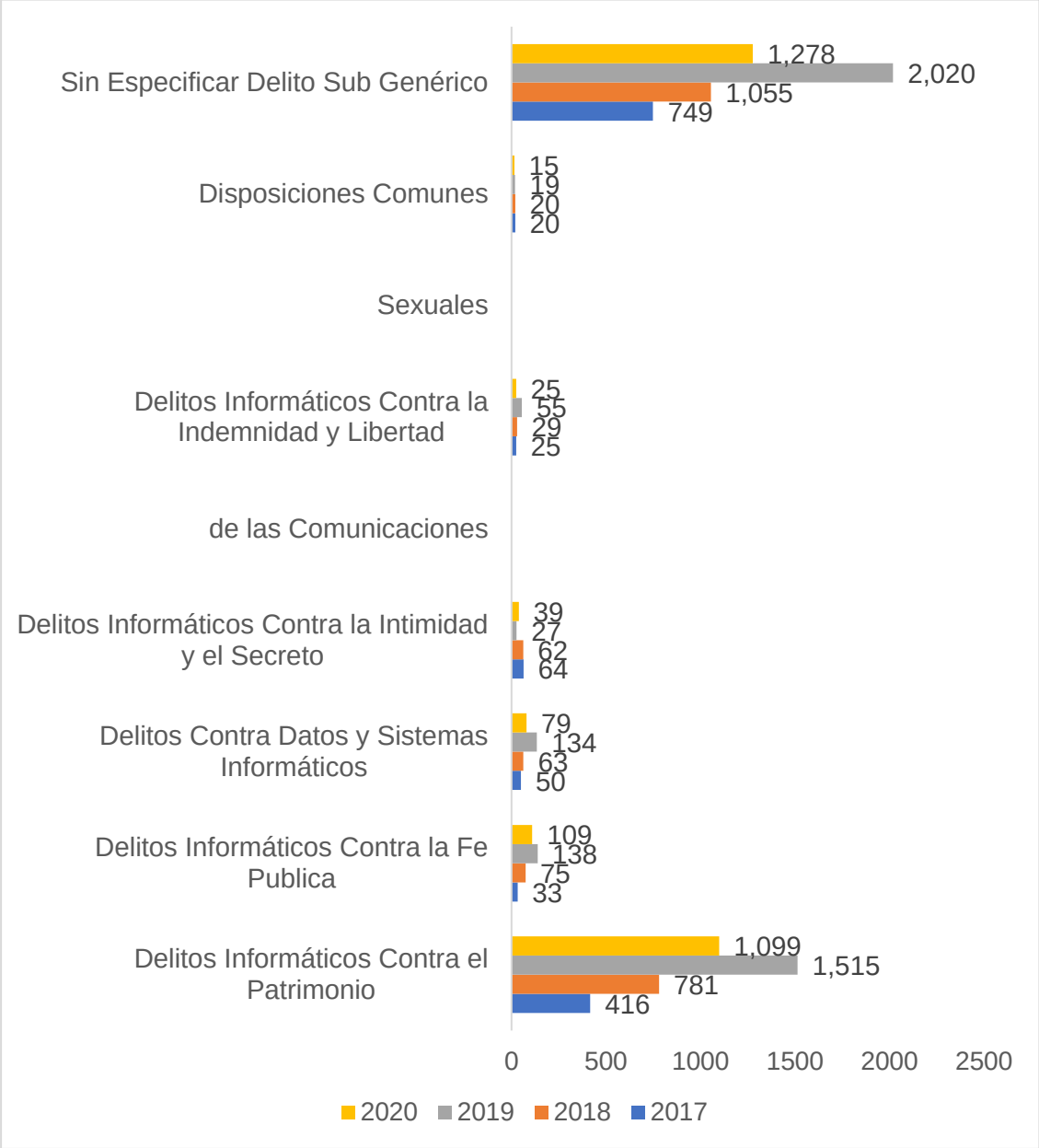
| Delitos Sub Genéricos | 2017 Enero-Julio | | 2018 Enero-Julio | | 2019 Enero-Julio | | 2020 Enero-Julio | | |
|---|---|---|---|---|---|---|---|---|---|
| | Nº Delitos | % | Nº Delitos | % | Nº Delitos | % | Nº Delitos | % | % Variación |
| Ley Nº 30096, Ley de Delitos Informáticos | | | | | | | | | |
| Delitos Informáticos Contra el Patrimonio | 416 | 30.66 | 781 | 37.46 | 1,515 | 38.77 | 1,099 | 41.57 | -27.46 |
| Delitos Informáticos Contra la Fe Publica | 33 | 2.43 | 75 | 3.60 | 138 | 3.53 | 109 | 4.12 | -21.01 |
| Delitos Contra Datos y Sistemas Informáticos | 50 | 3.68 | 63 | 3.02 | 134 | 3.43 | 79 | 2.99 | -41.04 |
| Delitos Informáticos Contra la Intimidad y el Secreto de las Comunicaciones | 64 | 4.72 | 62 | 2.97 | 27 | 0.69 | 39 | 1.48 | 44.44 |

| Delitos Sub Genéricos | 2017 Enero-Julio | | 2018 Enero-Julio | | 2019 Enero-Julio | | 2020 Enero-Julio | | |
|---|---|---|---|---|---|---|---|---|---|
| | Nº Delitos | % | Nº Delitos | % | Nº Delitos | % | Nº Delitos | % | Variación |
| Delitos Informáticos Contra la Indemnidad y Libertad Sexuales | 25 | 1.84 | 29 | 1.39 | 55 | 1.41 | 25 | 0.95 | -54.55 |
| Disposiciones Comunes | 20 | 1.47 | 20 | 0.96 | 19 | 0.49 | 15 | 0.57 | -21.05 |
| Sin Especificar Delito Sub Genérico | 749 | 55.20 | 1,055 | 50.60 | 2,020 | 51.68 | 1,278 | 48.32 | -36.73 |
| Total | 1,357 | 100.00 | 2,085 | 100.00 | 3,908 | 100.00 | 2,644 | 100.00 | -32.34 |

Nota: En el periodo de enero a julio de 2020, en el año 2020 hay una disminución en denuncias registradas en ciberdelitos, con respecto al periodo de enero a julio de 2019. Adaptado de:(Ministerio Público - Fiscalía de la Nación, Boletín Estadístico Julio 2018, 2018, pág. 54) y (Ministerio Público - Fiscalía de la Nación, Boletín Estadístico del Ministerio Público Julio 2020, 2020, pág. 48).

**Figura 22**

*Delitos Informáticos registrados en Fiscalías Penales y mixtas a nivel nacional en enero a julio 2017-2020*




Nota: En el periodo de enero a julio de 2020 hay una disminución en denuncias registradas en ciberdelitos, con respecto al periodo de enero a julio de 2019. Adaptado de: (Ministerio Público - Fiscalía de la Nación, Boletín Estadístico Julio 2018, 2018, pág. 54) y (Ministerio Público - Fiscalía de la Nación, Boletín Estadístico del Ministerio Público Julio 2020, 2020, pág. 48).

### C. El COVID y las ciberextorsiones

La pandemia del COVID-19 ha aumentado el uso de las tecnologías digitales en el Perú, por el trabajo remoto desde casa, necesidad de comunicación a distancia, comercio electrónico, clases virtuales, pero este aumento ha incrementado los delitos informáticos, entre ellos las ciberextorsiones.

"Perú registro más de 613 millones de intentos de ciberataque entre enero y junio de 2020, sumando al total de 15 mil millones de intentos en América Latina y el Caribe".(Fortinet Threat , 2020).

**Figura 23**

*Impacto del COVID por intentos de ciberataques*


Nota: En el primer semestre del año, el Perú obtuvo 613 millones de intentos de ciberataques. Adaptado de (Fortinet Threat , 2020).

Durante, el año 2020, durante la pandemia, ha aparecido nuevas modalidades de ciberataques, para realizar las ciberextorsiones para realizar las ciberextorsiones, entre ellas tenemos:

“El troyano bancario Trickbot, explota la temática del Covid-19 para distribuir malware mediante múltiples campañas de SPAM” (Presidencia del Consejo de Ministros & Secretaria de Gobierno Digital, Alerta Integrada de Seguridad Digital Nº 016-2020-PECERT, 2020, pág. 9). Este troyano es enviado por e-mail a cientos de usuarios, en un documento adjunto con la temática del COVID, con la supuesta prueba gratuita de COVID de una organización sin fines de lucro. Este troyano roba credenciales personales y otras credenciales con el fin de solicitar rescate a sus cibervíctimas.

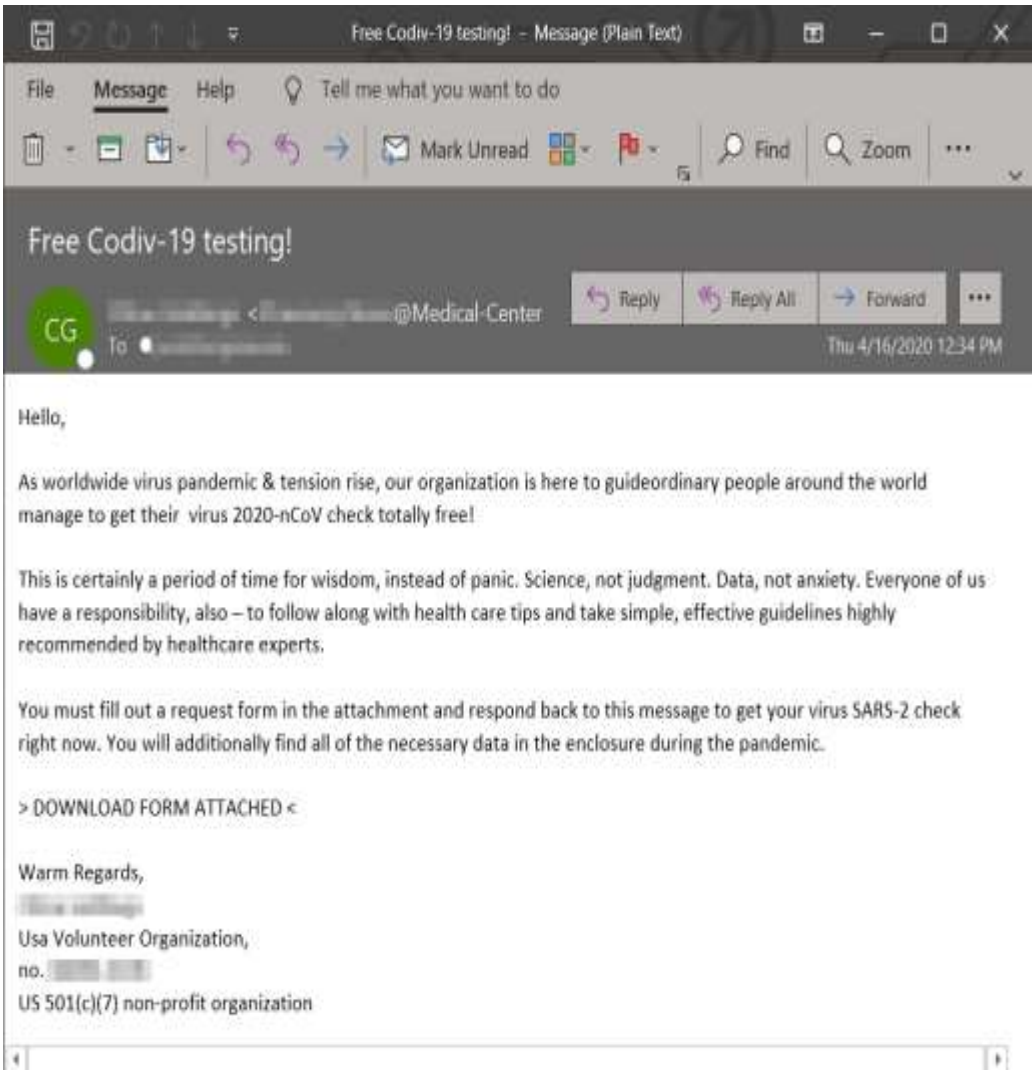
**Figura 24**

*Tweet: Microsoft Security Intelligence*


Nota: El troyano bancario Trickbot aparecido en el año 2020, durante la pandemia del COVID. Tomado de:(Presidencia del Consejo de Ministros & Secretaria de Gobierno Digital, Alerta Integrada de Seguridad Digital Nº 016-2020-PECERT, 2020).

**Figura 25**

*Correo malicioso usado por Trickbot*



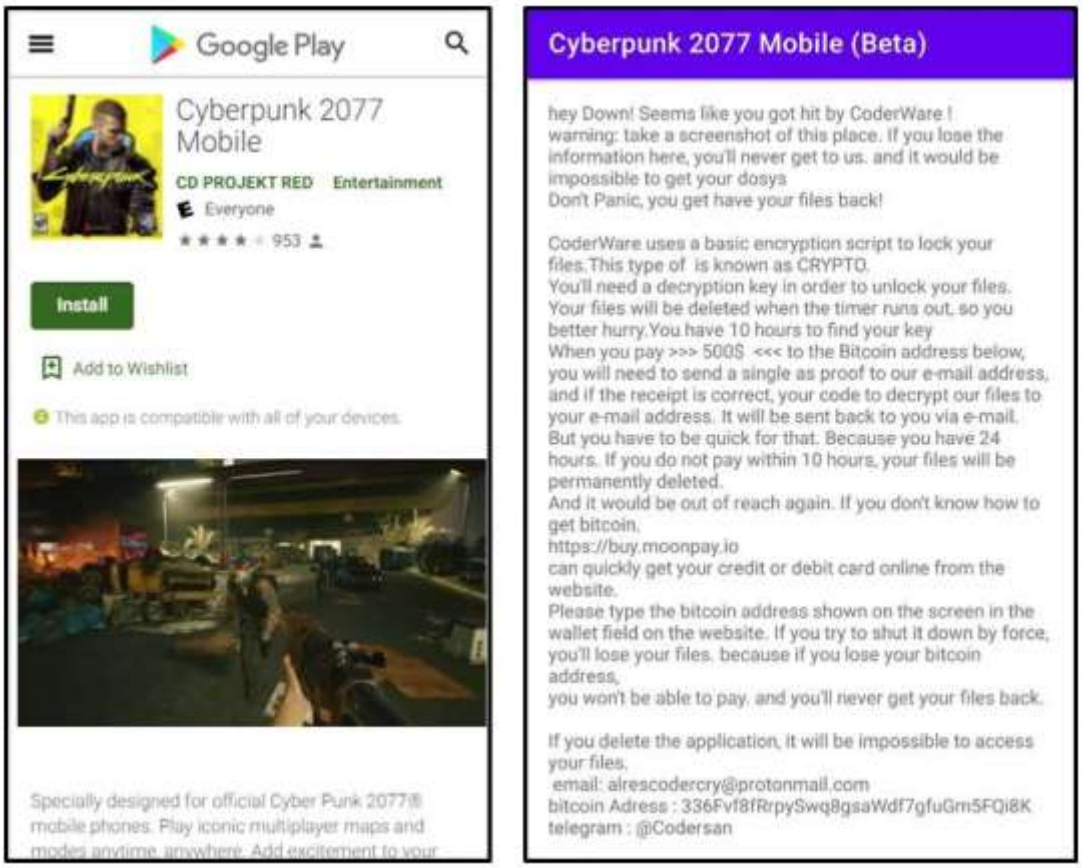

Nota: El troyano bancario Trickbot enviado por e-mail, aparecido en el año 2020, durante la pandemia del COVID. Tomado de: (Presidencia del Consejo de Ministros & Secretaria de Gobierno Digital, Alerta Integrada de Seguridad Digital Nº 016-2020-PECERT, 2020).

> “El 20 de diciembre de 2020, se detectó un nuevo ransomware denominado CoderWare, dirigido a aplicativos de juegos móviles, el cual se distribuye por medio de la plataforma de Google Play Store”. (Presidencia del Consejo de Ministros & Secretaria de Gobierno Digital, Alerta Integrada de Seguridad

Digital Nº 256-2020-PECERT, 2020, pág. 9). El CoderWare bloquea dispositivos móviles con el fin de bloquear, cifrar y encriptar los archivos para solicitar un rescate.

**Figura 26**

*Ransomware - CoderWare*




Nota: Ransomware - CoderWare aparecido en el año 2020, durante la pandemia del COVID. Tomado de (Presidencia del Consejo de Ministros & Secretaria de Gobierno Digital, Alerta Integrada de Seguridad Digital Nº 256-2020-PECERT, 2020).

### D. Dificultades que se presentan en las ciberextorsiones en el Perú

Entre las principales dificultades que se presentan para combatir las ciberextorsiones en el Perú, podemos mencionar:

- No se actualiza la Ley Nº 30096, conforme se va presentando nuevas modalidades de delitos informáticos, entre ellos las ciberextorsiones.

- No existe reglamento de la Ley Nº 30096, para aplicar de acuerdo a procedimientos específicos.
- No existe una Ley de Ciberseguridad en Perú, solo existe Política Nacional de Ciberseguridad Nacional del Perú.

Las siguientes dificultades que se detalla a continuación corresponde al informe Nº 105-DIRINCRI PNP/DIVINDAT/SEC, realizado por la DIVINDAT. (DIRINCRI PNP & DIVINDAT, 2019, págs. 3-4):

- Dentro de las investigaciones, las empresas de comunicaciones no entregan la información en forma oportuna, lo que ocasione el retraso de las investigaciones.
- Las entidades que investigan información sobre ciberataques, no comparten información. (DINI, ORI, DIGIMIN, etc).
- Las Fiscalías comunes, por el complejo que es el delito, no comprenden la forma en que se efectúa el delito.
- Las empresas, entidades, y personas no denuncian el delito informático de forma penal, por temor de afectar su imagen.
- Las penas de delitos informáticos son benignas y no persuasivas.
- Los delitos informáticos, se van innovando y requiere de personal calificado.

A continuación, las dificultades que detectaron el CONAPOC(Consejo Nacional de Política Criminal CONAPOC, 2020, págs. 60-63):

- Existe una brecha en la capacidad de persecución de los delitos informáticos, porque solo existen dos dependencias especializadas policiales en delitos informáticos en Lima y Arequipa, que no cubren la necesidad de asistir a las personas, e instituciones que son cibervíctimas.

- Las empresas proveedoras de servicios de comunicación e internet privadas, tienen deficientes mecanismos para obtener mantener registros de las direcciones IP de sus clientes.
- La información que brinda las empresas de servicios de comunicación e internet no es rápida; se desarrolla por medio de procesos como Levantamiento del Secreto de las comunicaciones, que deben ser expedidas por Resolución Judicial, por lo que impide que la persecución del ciberdelito sea eficaz.
- Todavía persiste no denunciar los ciberdelitos por parte de las personas e instituciones, lo cual se debe realizar acciones de sensibilizaciones para prevenir y denunciar los ciberdelitos.
- A pesar que existe normativa para los ciberdelitos, es necesario incorporar en las leyes y convenios, regulaciones que faciliten en forma oportuna, la información que requiere las autoridades encargadas de perseguir los ciberdelitos.
- No existe una estrategia clara a nivel nacional que brinde pautas de acción para hacer frente a los ciberdelitos.
- La Policía Nacional del Perú no cuenta con investigación sobre ciberdelitos, sin embargo, si tiene cursos de capacitación continua en ciberdelitos, desarrollados por la Escuela de Investigación Criminal.
- No existe una capacitación de personal permanente entre las entidades nacionales e internacional, en ciberdelitos.
- Existen deficiencias en el Equipo de Respuesta ante Emergencias Informáticas (CSIRT), por la falta de capacitación permanente y actualizada.
- Existe carencia de un cuerpo especializado de peritos informáticos en el Ministerio Público, que brinde apoyo a las fiscalías a nivel nacional.
- A nivel nacional, existe poca capacitación a los fiscales sobre injerencias de las Tecnologías de la Información y la Comunicación (TICs) en la

comisión de delitos informáticos, cooperación judicial internacional respecto al requerimiento de conservación de datos informáticos.

- Falta software de última generación, especializado y herramientas informáticas forenses para las pericias informáticas e investigaciones sobre los ciberdelitos.
- No hay convenios suficientes con empresas tecnológicas nacional e internacional para que proveen con el Estado recursos tecnológicos suficientes para combatir los ciberdelitos.
- No hay implementación de manuales estandarizados de cooperación internacional para formular pedidos de asistencia judicial a países extranjeros.
- Falta la implementación de un laboratorio forense con personal especializado en ciberdelitos, con equipos tecnológicos modernos y actualizados.
- Es insuficiente la cultura de difusión, prevención de los ciberdelitos por medios de comunicación masiva.

### *10. Sugerencia para combatir las ciberextorsiones*

Conociendo las dificultades que se presentan en las ciberextorsiones que forma parte de los delitos informáticos, en el Perú, por la no existencia de un área especializada en delitos informáticos, que es de interés público, nacional, necesario, sugiero “La creación de Fiscalías y Juzgados Especializados de Delitos Informáticos”, mediante la creación de una Ley, conforme el artículo 107º de la Constitución Política del Perú, para que de esta manera se comba eficazmente los ciberdelitos.

Para que no exista un desequilibrio presupuestal, según los artículos 77ª y 78ª de la Constitución Política del Perú, el financiamiento estaría a cargo del Ministerio Público. A la vez se estaría dando cumplimiento al Convenio de Budapest, beneficiando todos los peruanos en su bienestar e integridad económica, social, e individual.

## 3.5 Hipótesis

### 1. General

La existencia de un área especializada en Delitos Informáticos que este contemplada dentro de la Ley Nº 30096 de Delitos Informáticos, que unifique procedimientos, métodos en materia de ciberdelitos; que prevenga y sancione los delitos informáticos, va disminuir la ineficacia de la Ley Nº 30096 de Delitos Informáticos.

### 2. Específicos

- Los métodos, técnicas, herramientas perfeccionadas y sofisticas que usan los grupos organizados de ciberextorsionadores han contribuido al aumento de las ciberextorsiones.
- Las herramientas logísticas de la DIVINDAT para combatir las ciberextorsiones no son adecuadas.
- La ley 30096 de Delitos Informáticos no se ha reglamentado.
- La ley 30096 de Delitos Informáticos no se actualizado conforme el avance de nuevos ciberdelitos.
- La ley 30096 de Delitos Informáticos no se adecuado al convenio de Budapest.

## 3.6 Variables

- **Variable independiente (VI):** Ineficacia de la Ley Nº 30096 de Delitos Informáticos.
- **Variable dependiente (VD):** La existencia de un área especializada en Delitos Informáticos.

## 3.7 Definición operacional de términos

- **Ciberdelito:** es un término que hace referencia a la actividad delictiva a través del Internet.
- **Ciberextorsión:** es el delito cometido por una persona mediante el uso de medios informáticos en perjuicio de su víctima a través de la web.

- **Ciberdelincuencia:** es aquella actividad que por medio de un sistema informático tiene como objetivo atentar contra la confidencialidad, integridad, disponibilidad del uso fraudulento de los sistemas informáticos, redes y datos.
- **Cibercriminales:** son aquellos sujetos que pueden infectar los ordenadores con virus y malware para dañar dispositivos para que estos dejen de funcionar o puedan ser manipularlos.
- **Ciberamenazas:** son aquellas realizadas por cualquier medio de comunicación tecnológico en la red (whatsapp, facebook, instagram, correos electrónicos, etc.).
- **Cibercrimen:** es aquel que utiliza ordenadores para cometer delitos mediante el uso de ordenadores, redes para propagar malware, información ilegal y delitos informáticos.
- **Ciberseguridad:** es la práctica realizada para defender computadores, servidores, dispositivos móviles, sistemas electrónicos, redes y datos contra ataques maliciosos.
- **Convenio Budapest:** es el primer tratado internacional que busca hacer frente a los delitos informáticos y busca combatir la ciberdelincuencia (delitos en Internet) entre sus naciones firmantes.
- **DIVINDAT:** es la División de Investigación de Delitos de Alta Tecnología de la DIRINCRI – PNP que se encarga de patrullar el ciberespacio de los peruanos.
- **Ciberespacio:** es el ámbito de la información en la que se encuentran nuestros ordenadores y las redes digitales de todo el mundo.

# CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN

## 3.1 Diseño metodológico

### 3.1.1 Tipo de investigación

La presente investigación está dentro de una Investigación Básica, Jurídica, con nivel descriptivo que busca evaluar el conocimiento que se obtiene sobre el tipo penal de los delitos informáticos en su modalidad de ciberextorsión.

### 3.1.2 Nivel de investigación

El nivel de investigación es descriptivo, causal y explicativa porque su propósito es dar una solución al problema sobre la ineficacia en la aplicación de la Ley 30096 Delitos Informáticos sobre ciberextorsión en el Perú.

## 3.2 Población y muestra

- **Universo/Población:**

  N = 15 agentes de la DIVINDAT del departamento Investigación de Delitos Informáticos y 19 Fiscales superiores especializados contra la Criminalidad Organizada de Lima, haciendo un total de 34 personas.

  N= 32 personas especializadas en Delitos Informáticos (Población Objetiva).

- ***Muestra:***

  Tamaño de muestra: 32 personas.

  Margen de error: 5%

  Nivel de Confianza: 95%

  Muestreo: Probabilístico, al azar simple.

- **Determinación de la muestra.**

  Datos:

  Margen de error: 5%

  Tamaño de la Población: 34

  Nivel de Confianza, valores Z:95%

Varianza (valor para reemplazar en la fórmula):1.960

**Ecuación 1**

*Fórmula tamaño de la muestra*

$$\frac{N^*(\alpha_c * 0{,}5)^2}{1+(e^2*(N-1))} =$$

**Donde:**

- $\alpha_c$ = Valor del nivel de confianza (varianza).
- **Nivel de confianza**, riesgo que se acepta al equivocarse cuando se presenta los resultados.
- $e$ = Margen de error.
- **Margen de error**, es el error que se acepta de equivocarse al seleccionar una muestra.
- $N$ = Tamaño Población (universo).

Reemplazando datos en la fórmula:

**Ecuación 2**

*Cálculo de la muestra*

$$\frac{34(1.960 * 0.5)^2}{1 + (0.05^2 * (34 - 1)}$$

= 32 personas

### 3.3 Técnicas e instrumentos de recolección de datos

Se emplea la encuesta como técnica de procesamiento de datos.

### 3.4 Diseño de recolección de datos

Se utilizará el diseño no experimental de tipo descriptivo, causal y explicativa.

### 3.5 Procesamiento y análisis de datos

El Procesamiento y análisis datos, la recopilación es relevante e importante,

obtenidos en libros, revistas, manuales e información de páginas web; también se realiza la técnica de encuesta, utilizando como instrumento cuestionarios a especialistas en juzgados penales y agentes de la DIVINDAT.

Se analizó, describió, se sintetizó toda la información, se realizó cuadros, gráficos estadísticos con los resultados obtenidos de los cuestionarios; se elaboró una propuesta al problema de la investigación, finalmente se realizó las conclusiones y recomendaciones, con el fin de obtener una investigación de utilidad para futuras investigaciones similares.

## 3.6 Aspectos Éticos

La presente investigación está de acuerdo al Código de Ética de Investigación de la Universidad Privada San Juan Bautista, Resolución Nº 471-2019-CU-UPSJB, del 17-09-2019; tomando en cuenta los siguientes principios éticos:

- **Respeto:** Se respetó los derechos, bienestar de los participantes de estudio de investigación, quienes tienen el derecho de decidir su participación en estudios de investigación y expresar esa voluntad.
- **Justicia:** Se aseguró que todos los beneficios, compromisos sean iguales para todos los participantes, sin distinción de raza, ingreso económico, procedencia, género u cualquier condición.
- **Beneficencia:** Se aseguró que la investigación este de acorde con el nivel del conocimiento científico alcanzado sobre el tema a la fecha, que el diseño de estudio es el conveniente para el propósito y objetivo de la investigación.

# CAPÍTULO IV: ANÁLISIS DE LOS RESULTADOS

## 4.1Resultados

La presente información, fue obtenida a través de la aplicación del instrumento llamado cuestionario, el cual se formularon 10 preguntas Dicotómica 1(si) 2(No), de acuerdo a los indicadores de las variables; que fueron respondidas por 14 Agentes de la DIVINDAT del departamento de Delitos informáticos, y 18 Fiscales Superiores Especializados contra la Criminalidad Organizada de Lima, haciendo un total de 32 cuestionarios realizados.

**Pregunta 1:** ¿Existe en el Perú grupos organizados de ciberextorsionadores?

**Tabla 9**

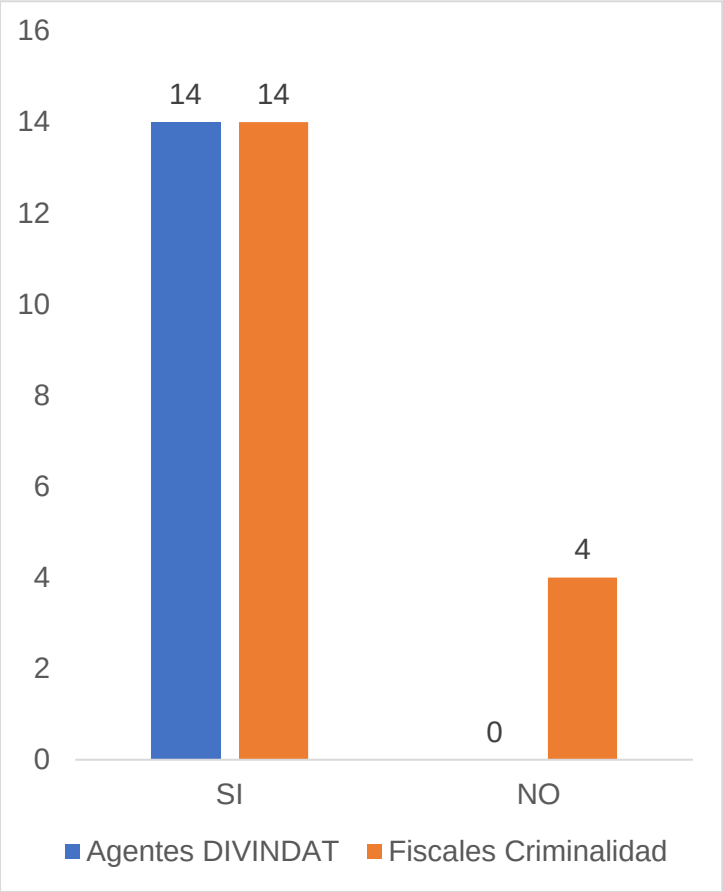
*Existencia de grupos organizados de ciberextorsionadores*

| **Item** | **Encuestados** | | | | **Total** | |
|---|---|---|---|---|---|---|
| | Agentes DIVINDAT | | FiscalesCriminalidad | | | |
| | Frecuencia | Porcentaje | Fecuencia | Porcentaje | Frecuencia | Porcentaje |
| **Si** | 14 | 44% | 14 | 44% | 28 | 88% |
| **No** | 0 | 0% | 4 | 13% | 4 | 13% |
| **Total** | 14 | 44% | 18 | 56% | 32 | 100% |

Nota: Elaboración propia

**Figura 27**

*Existencia de grupos organizados de ciberextorsionadores*




Nota: Elaboración propia.

**Interpretación:** Los resultados indican, según los encuestados que el 88% afirmaron que existe en el Perú grupos organizados de ciberextorsionadores, mientras que el 13% indican lo contrario, siendo este 13% la respuesta de los Fiscales Especializados contra la Criminalidad Organizada de Lima.

**Pregunta 2:** En comparación con años anteriores: ¿Las ciberextorsiones están en aumento?

**Tabla 10**

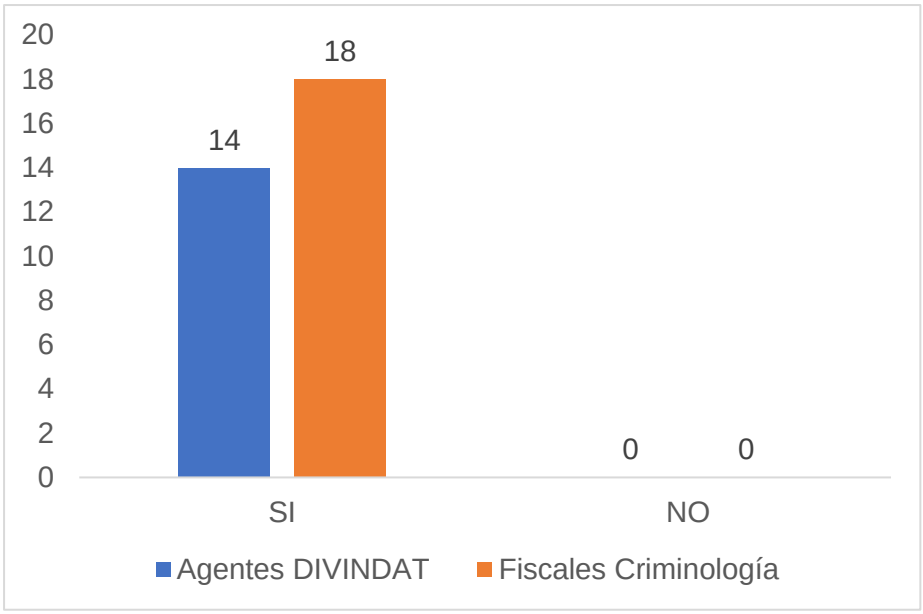
*Aumento de las ciberextorsiones 2016-2019*

| Item | Encuestados | | | | Total | |
|---|---|---|---|---|---|---|
| | Agentes DIVINDAT | | FiscalesCriminalidad | | | |
| | Frecuencia | Porcentaje | Fecuencia | Porcentaje | Frecuencia | Porcentaje |
| **Si** | 14 | 44% | 18 | 56% | 32 | 100% |
| **No** | 0 | 0% | 0 | 0% | 0 | 0% |
| **Total** | 14 | 44% | 18 | 56% | 32 | 100% |

Nota: Elaboración propia

**Figura 28**

*Aumento de las ciberextorsiones 2016-2019*




Nota: Elaboración propia.

**Interpretación:** Los resultados indican, según los encuestados que al 100% han afirmado que las ciberextorsiones están en aumento en comparación con años anteriores. Tanto los Agentes de la DIVINDAT del departamento de Delitos Informáticos, y los Fiscales Superiores Especializados contra la Criminalidad Organizada de Lima han afirmado en forma absoluta. Esta comparación comprende los años 2016, 2017, 2018 y 2019.

**Pregunta 3:** ¿Conoce los diversos métodos, técnicas o herramientas que utilizan los ciberextorsionadores?

**Tabla 11**

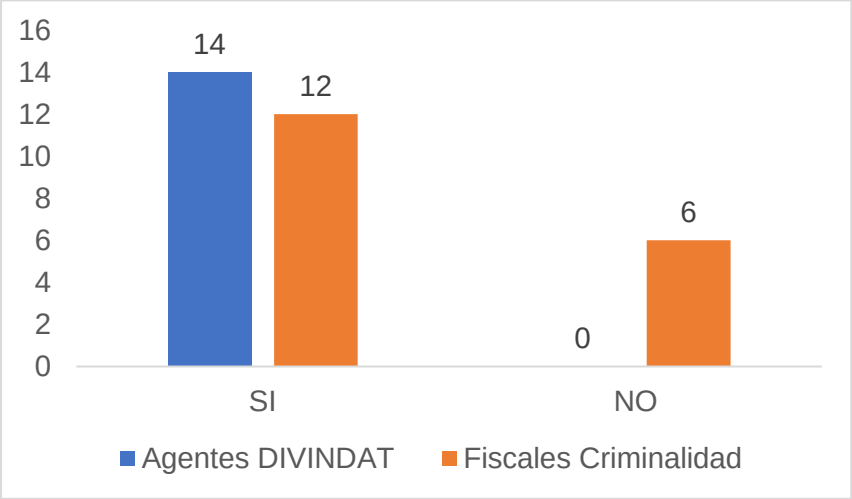
*Conocimiento de métodos, técnicas o herramientas de ciberextorsión*

| **Item** | **Encuestados** | | | | **Total** | |
|---|---|---|---|---|---|---|
| | Agentes DIVINDAT | | FiscalesCriminalidad | | | |
| | Frecuencia | Porcentaje | Fecuencia | Porcentaje | Frecuencia | Porcentaje |
| **Si** | 14 | 44% | 12 | 38% | 26 | 81% |
| **No** | 0 | 0% | 6 | 19% | 6 | 19% |
| **Total** | 14 | 44% | 18 | 56% | 32 | 100% |

Nota: Elaboración propia

**Figura** **29**

*Conocimiento de métodos, técnicas o herramientas de ciberextorsionadores*




Nota: Elaboración propia.

**Interpretación:** Los resultados indican, según los encuestados que el 81% afirma conocer los diversos métodos, técnicas o herramientas que utilizan los ciberextorsionadores, mientras que el 19% conformado por Fiscales Superiores Especializados contra la Criminalidad Organizada de Lima, desconocen los diversos métodos, técnicas o herramientas que utilizan los ciberextorsionadores.

**Pregunta 4:** La DIVINDAT: ¿Cuenta con herramientas logísticas para combatir la ciberextorsión?

**Tabla 12**

*Herramientas logísticas para combatir la ciberextorsión*

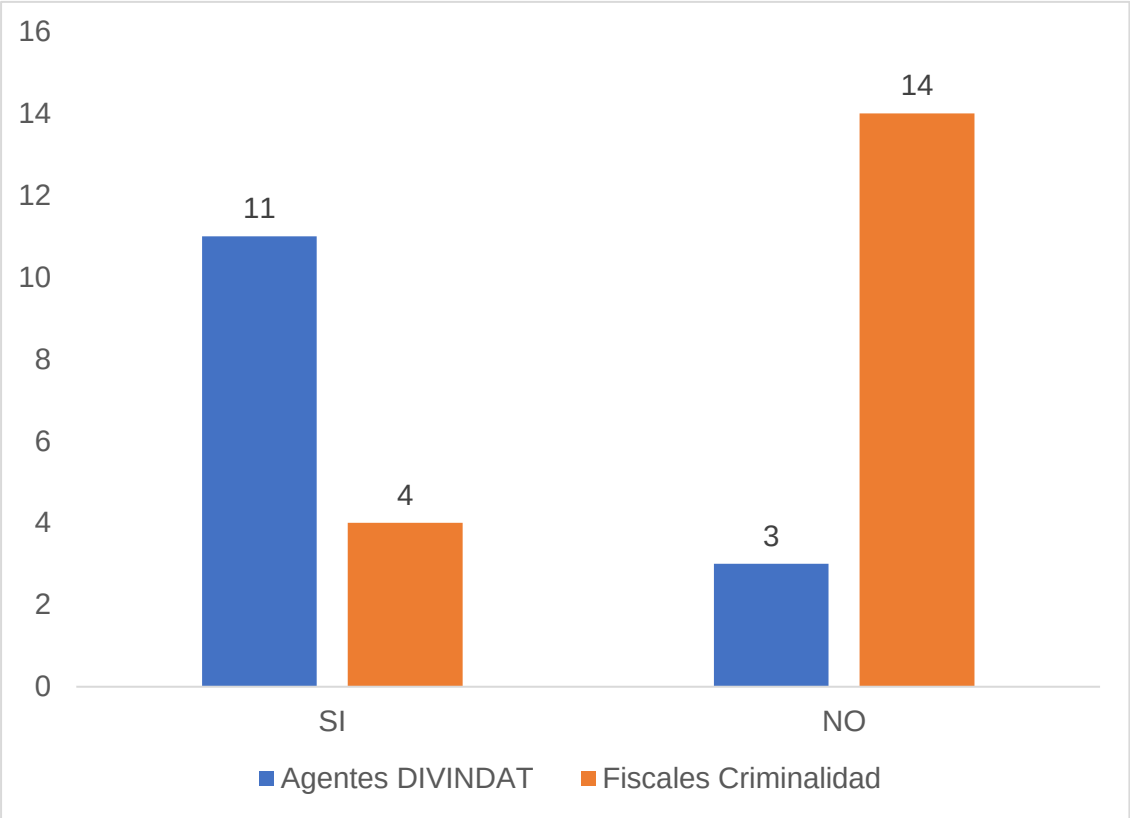
| **Item** | **Encuestados** | | | | **Total** | |
|---|---|---|---|---|---|---|
| | Agentes DIVINDAT | | FiscalesCriminalidad | | | |
| | Frecuencia | Porcentaje | Fecuencia | Porcentaje | Frecuencia | Porcentaje |
| **Si** | 11 | 34% | 4 | 13% | 15 | 47% |
| **No** | 3 | 9% | 14 | 44% | 17 | 53% |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Total** | 14 | 44% | 18 | 56% | 32 | 100% |

Nota: Elaboración propia

**Figura 30**

*Herramientas logísticas para combatir la ciberextorsión*




Nota: Elaboración propia.

**Interpretación: Los** resultados indican, según los encuestados que el 47% afirma que la DIVINDAT cuenta con herramientas logísticas para combatir la ciberextorsión, mientras que el porcentaje mayor que es el 53% señala que la DIVINDAT no cuenta con herramientas logísticas para combatir la ciberextorsión.

**Pregunta 5:** ¿Es positivo el rol que desempeña la DIVINDAT en la lucha contra delitos de ciberextorsión?

**Tabla 13**

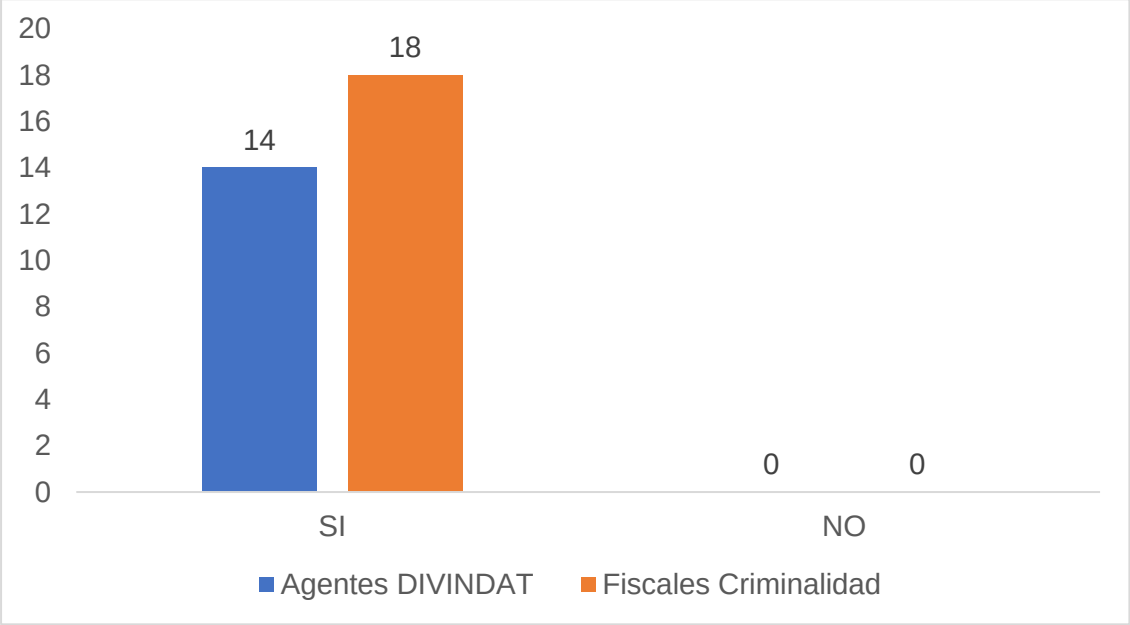
*Rol que desempeña la DIVINDAT*

| Item | Encuestados | | | | Total | |
|---|---|---|---|---|---|---|
| | Agentes DIVINDAT | | FiscalesCriminalidad | | | |
| | Frecuencia | Porcentaje | Fecuencia | Porcentaje | Frecuencia | Porcentaje |
| **Si** | 14 | 44% | 18 | 56% | 32 | 100% |
| **No** | 0 | 0% | 0 | 0% | 0 | 0% |
| **Total** | 14 | 44% | 18 | 56% | 32 | 100% |

Nota: Elaboración propia

**Figura 31**

*Rol que desempeña la DIVINDAT*




Nota: Elaboración propia.

**Interpretación:** Los resultados indican, según los encuestados que al 100% han afirmado que es positivo el rol que desempeña la DIVINDAT en la lucha contra delitos de ciberextorsión. Tanto los Agentes de la DIVINDAT del departamento de Delitos Informáticos, y los Fiscales Superiores Especializados contra la Criminalidad Organizada de Lima han afirmado en forma absoluta.

**Pregunta 6:** ¿Existe especialistas en materia de delito de ciberextorsión para la aplicación de la ley N° 30096 y sus modificatorias?

**Tabla 14**

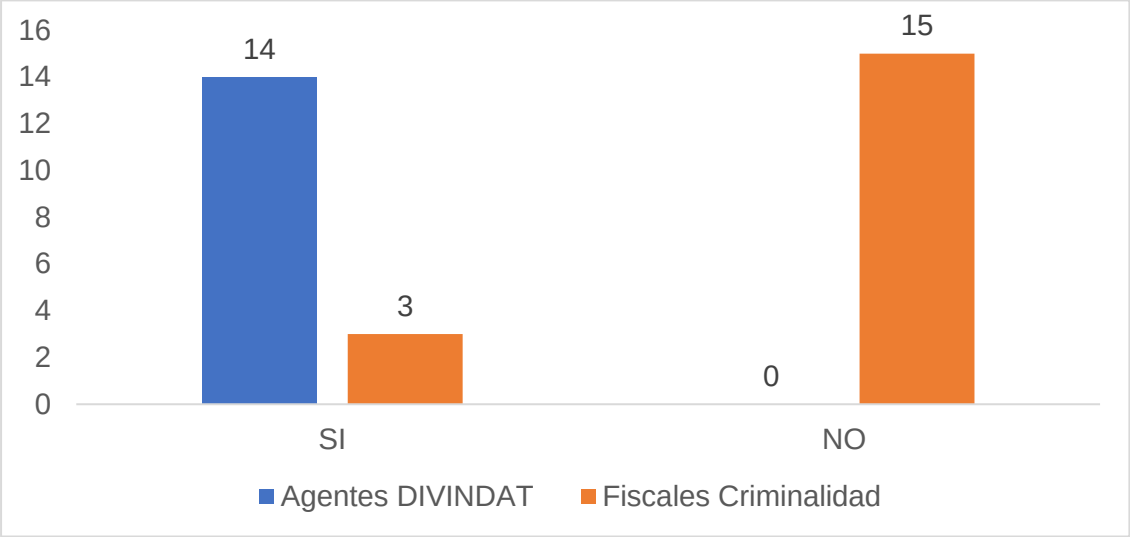
*Especialistas en materia de delito de ciberextorsión*

| **Item** | **Encuestados** | | | | **Total** | |
|---|---|---|---|---|---|---|
| | Agentes DIVINDAT | | FiscalesCriminalidad | | | |
| | Frecuencia | Porcentaje | Fecuencia | Porcentaje | Frecuencia | Porcentaje |
| **Si** | 14 | 44% | 3 | 9% | 17 | 53% |
| **No** | 0 | 0% | 15 | 47% | 15 | 47% |
| **Total** | 14 | 44% | 18 | 56% | 32 | 100% |

Nota: Elaboración propia

**Figura 32**

*Especialistas en materia de delito de ciberextorsión*




Nota: Elaboración propia.

**Interpretación:** Los resultados indican, según los encuestados que el 53% afirma que existe especialistas en materia de delito de ciberextorsión para la aplicación de la ley N° 30096 y sus modificatorias, y el 47% afirma lo contrario, siendo este 47% la respuesta de los Fiscales Especializados contra la Criminalidad Organizada de Lima.

**Pregunta 7:** ¿Existen factores que impidan la aplicación de la Ley N°30096 y sus modificatorias en el delito de ciberextorsión?

**Tabla 15**

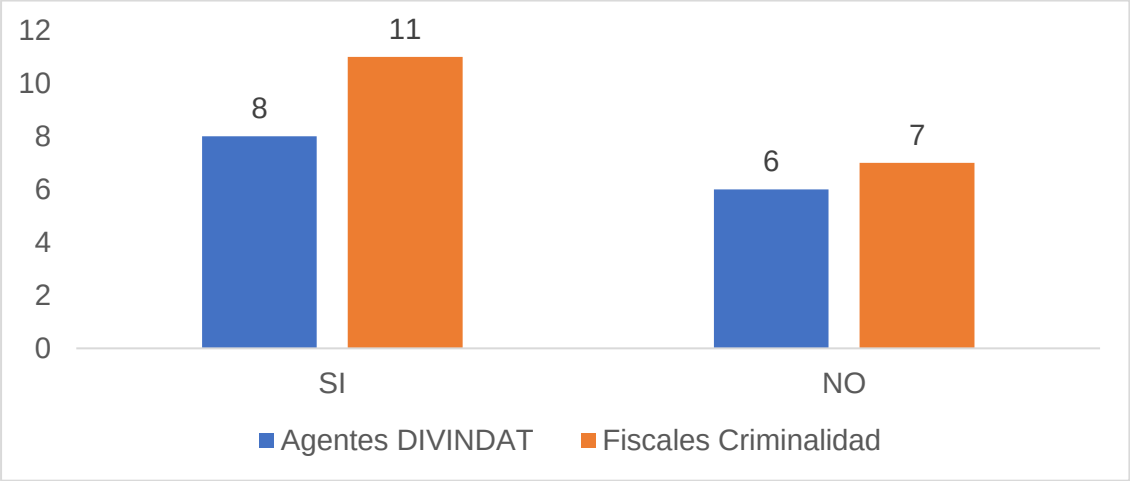
*Factores que impiden la interpretación de la Ley Nº 30096*

| **Item** | **Encuestados** | | | | **Total** | |
|---|---|---|---|---|---|---|
| | Agentes DIVINDAT | | FiscalesCriminalidad | | | |
| | Frecuencia | Porcentaje | Fecuencia | Porcentaje | Frecuencia | Porcentaje |
| **Si** | 8 | 25% | 11 | 34% | 19 | 59% |
| **No** | 6 | 19% | 7 | 22% | 13 | 41% |
| **Total** | 14 | 44% | 18 | 56% | 32 | 100% |

Nota: Elaboración propia

**Figura 33**

*Factores que impiden la aplicación de la Ley Nº 30096*




Nota: Elaboración propia.

**Interpretación:** Los resultados de este cuadro indican, según los encuestados que el 59% afirma que si existen factores que impidan la aplicación de la Ley N°30096 y sus modificatorias en el delito de ciberextorsión, mientras que el 41% afirma lo contrario.

**Pregunta 8:** ¿Existe transgresiones de la ley N° 30096 y sus modificatorias en el delito de ciberextorsión?

**Tabla 16**

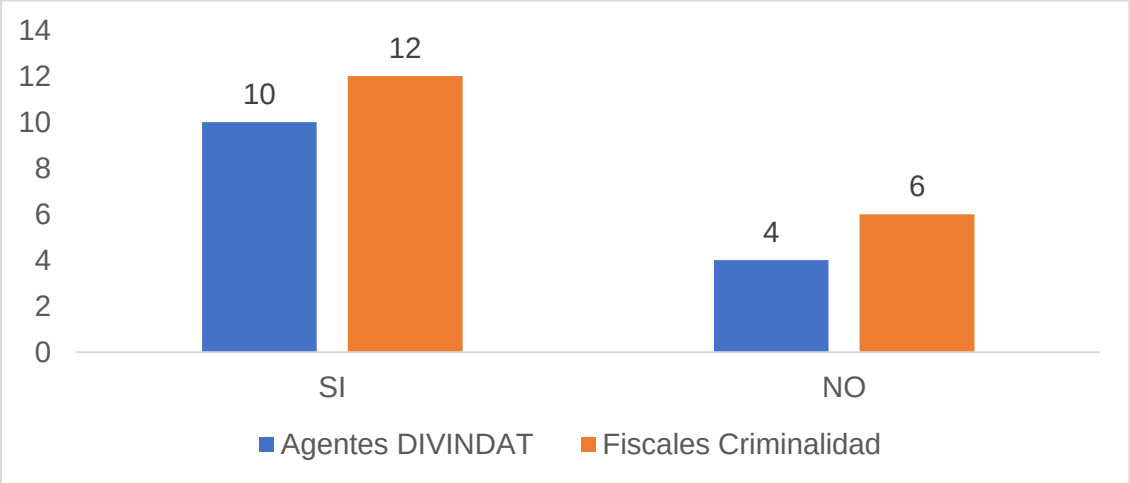
*Transgresión de la Ley Nº 30096 en el delito de ciberextorsión*

| **Item** | **Encuestados** | | | | **Total** | |
|---|---|---|---|---|---|---|
| | Agentes DIVINDAT | | FiscalesCriminalidad | | | |
| | Frecuencia | Porcentaje | Fecuencia | Porcentaje | Frecuencia | Porcentaje |
| **Si** | 10 | 31% | 12 | 38% | 22 | 69% |
| **No** | 4 | 13% | 6 | 19% | 10 | 31% |
| **Total** | 14 | 44% | 18 | 56% | 32 | 100% |

Nota: Elaboración propia

**Figura 34**

*Transgresión de la Ley Nº 30096 en el delito de ciberextorsión*




Nota: Elaboración propia.

**Interpretación:** Los resultados indican, según los encuestados que el 69% afirma que si existe transgresiones de la Ley N° 30096 y sus modificatorias en el delito de ciberextorsión, mientras que el 31% afirma lo contrario.

**Pregunta 9:** ¿Ha sido la ley N°30096 y sus modificatorias en el delito de ciberextorsión, materia de estudio en charlas, talleres o capacitaciones?

**Tabla 17**

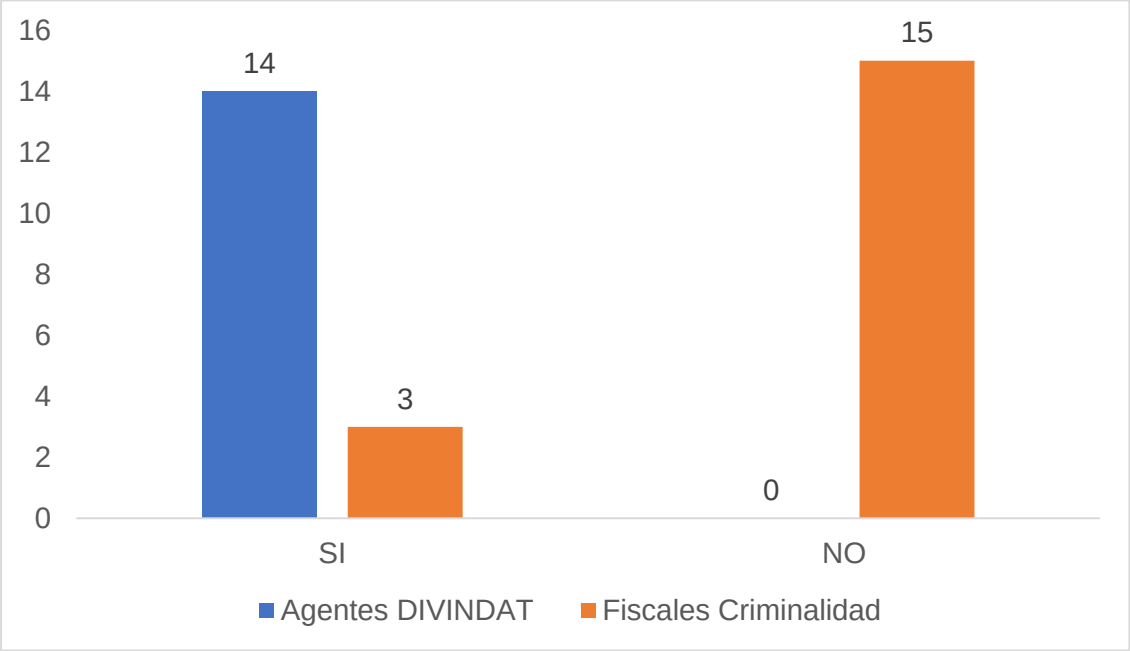
*La Ley Nº 30096 en materia de estudio en charlas, talleres o capacitaciones*

| **Item** | **Encuestados** | | | | **Total** | |
|---|---|---|---|---|---|---|
| | Agentes DIVINDAT | | FiscalesCriminalidad | | | |
| | Frecuencia | Porcentaje | Fecuencia | Porcentaje | Frecuencia | Porcentaje |
| **Si** | 14 | 44% | 3 | 9% | 17 | 53% |
| **No** | 0 | 0% | 15 | 47% | 15 | 47% |
| **Total** | 14 | 44% | 18 | 56% | 32 | 100% |

Nota: Elaboración propia

**Figura 35**

*La Ley Nº 30096 en materia de estudio en charlas, talleres o capacitaciones*




Nota: Elaboración propia.

**Interpretación:** Los resultados indican, según los encuestados que el 53% afirma que ha sido la ley N°30096 y sus modificatorias en el delito de ciberextorsión, materia de estudio en charlas, talleres o capacitaciones, mientras que el 47% afirma lo contrario, siendo este 47% la respuesta de los Fiscales Especializados contra la Criminalidad Organizada de Lima.

**Pregunta 10:** ¿El convenio de Budapest es un factor principal para la aplicación de la Ley N° 30096 y sus modificatorias?

**Tabla 18**

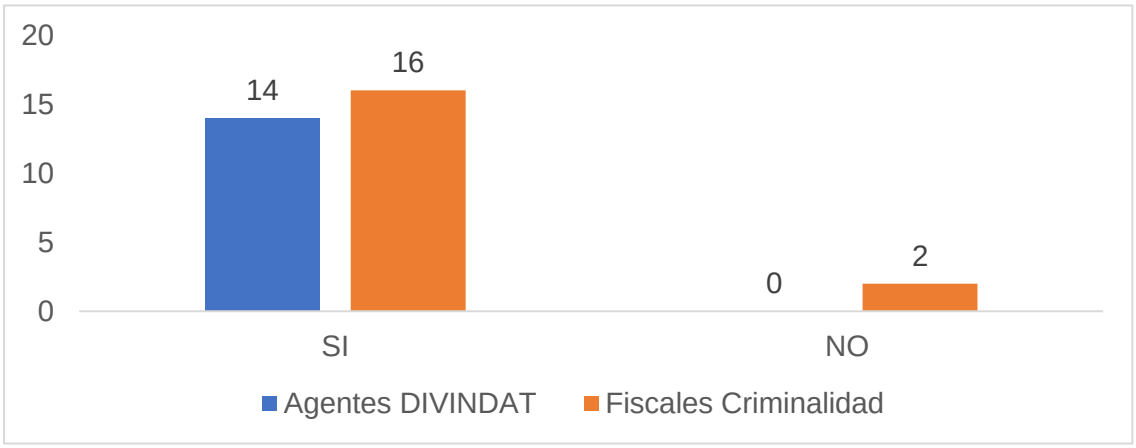
*El convenio de Budapest como factor principal para la aplicación de la Ley Nº 30096*

| Item | Encuestados | | | | Total | |
|---|---|---|---|---|---|---|
| | AgentesDIVINDAT | | FiscalesCriminalidad | | | |
| | Frecuencia | Porcentaje | Fecuencia | Porcentaje | Frecuencia | Porcentaje |
| **Si** | 14 | 44% | 16 | 50% | 30 | 94% |
| **No** | 0 | 0% | 2 | 6% | 2 | 6% |
| **Total** | 14 | 44% | 18 | 56% | 32 | 100% |

Nota: Elaboración propia

**Figura 36**

El convenio de Budapest como factor principal para la aplicación de la Ley Nº 30096




Nota: Elaboración propia.

**Interpretación:** Los resultados de este cuadro indica, según los encuestados que el 94% afirma que el convenio de Budapest es un factor principal para la aplicación de la Ley Nº 30096 y sus modificatorias, mientras que el 6% afirma lo contrario, siendo este 6% la respuesta de los Fiscales Especializados contra la Criminalidad Organizada de Lima.

## 4.2Discusión

Después de haber elaborado los resultados de la investigación sobre la falta de eficacia de la ley Nº 30096 de Delitos Informáticos en su aplicación para el delito de ciberextorsión en el Perú, con empleo de los datos encontrados en el curso de la investigación de campo y habiendo realizado un análisis estadístico; se encontró la discusión de los principales hallazgos, comprobando la hipótesis general: La existencia de un área especializada en Delitos Informáticos que este contemplada dentro de la Ley Nº 30096 de Delitos Informáticos, que unifique procedimientos, métodos en materia de ciberdelitos; que prevenga y sancione los delitos informáticos, va disminuir la ineficacia de la Ley Nº 30096 de Delitos Informáticos.

Para lo cual analizaré las variables independientes y variable dependiente, con trabajos previos de investigación, contrastados con los resultados obtenidos, para conocer si se ha logrado alcanzar los objetivos propuestos.

- **Variable Independiente:** Ineficacia de la Ley Nº 30096 de Delitos Informáticos.
- **Supuesto:** Se puede decir que si se presenta ineficacia de la ley Nº 30096 para las ciberextorsiones en el Perú; ya que no existe una reglamentación especializada sobre delitos informáticos en la toma de acciones para combatir las ciberextorsiones, porque de acuerdo a los resultados obtenidos, en el Perú existe grupos organizados de ciberextorsionadores que operan a nivel nacional, e internacional, convirtiéndose las ciberextorsiones en el negocio delincuencial informático de mayor auge hasta la actualidad por su crecimiento acelerado e innovador; ya que existen nuevos métodos, técnica o herramientas que son usadas para cometer las ciberextorsiones, aunque consideran que la DIVINDANT realiza un trabajo adecuado y conforme a la ley Nº 30096, cumpliendo un rol importante contra la lucha de las ciberextorsiones, las ciberextorsiones continúan siendo perjudicial en el bienestar de la sociedad peruana.

Los grupos organizados de ciberdelincuentes, como la ciberdelincuencia, como coindice Morales Delgado (2016), está en crecimiento, y como coincide Tenorio Pereyra (2018) están en constante evolución.

Los grupos organizados de ciberdelincuentes, poseen una estructura cibercriminal muy organizada, como coincide Mateos Pascual (2013).

El aumento de ciberextorsionadores y ciberextorsiones, como coincide Ruiz Cruz(2016) se ha dado porque el uso de los medios informáticos ha aumentado, es por eso que como coincide Mateos Pascual (2013)**,** que los ciberdelincuentes han encontrado un lugar de posibilidades para cometer sus ciberdelitos.

Es asi como coincide Cárdenas Gallardo & Lazo Fernández (2014), que las TIC's son una de las grandes herramientas para cometer los ciberdelitos.

Los ciberdelincuentes no se estancan en un único perfil, si no que utiliza diversos métodos, herramientas modernas y actualizadas, como coincide Mateos Pascual (2013).

Con lo que respecta a la DIVINDAT, su rol contra los delitos infornáticos es positivo, asi como coincide Cárdenas Gallardo & Lazo Fernández (2014), pero no tiene las herrramientas logísticas, apoyo inmediato de empresas de comunicación como coincide el informe Nº 105-DIRINCRI PNP/DIVINDAT/SEC, realizado por la DIVINDAT. (2019).
Así mismo la DIVINDAT tiene déficit en su personal y no cuenta con instrumentos tecnológicos suficientes como coinciden Cárdenas Gallardo & Lazo Fernández (2014), lo cual pone en riesgo el cumplimiento de su misión.

De lo anterior mencionado, se debe que la ley Nº 30096, no cuenta con una reglamentación especializada en delitos informáticos, en donde exprese todas

las pautas y procedimientos para combatir los delitos.

- **Variable Dependiente:** La existencia de un área especializada en Delitos Informáticos.
- **Supuesto:** Se puede decir que no existen prevenciones, ni sanciones adecuadas para la ciberextorsión ya que todavía falta implementar un área especializada sobre los delitos informáticos y que aplique medidas a la ciberextorsión; por lo cual de acuerdo a los resultados obtenidos todavía no hay un número mayoritario de especialistas en materia del delito de la ciberextorsión para que aplique de manera eficiente y de acuerdo las medidas preventivas y sancionadoras; a pesar que si existe capacitación, talleres, charlas teniendo como materia de estudio la Ley Nº 30096 y sus modificatorias, tampoco existe un número mayoritario de personas con capacidad en forma continua, actualizadas de acuerdo al avance de la ciberextorsiones; por lo que va generar transgresiones, factores que van impedir la aplicación en forma eficaz de la ley Nº 30096 y sus modificatorias. Asimismo, cabe resaltar que en el Perú el convenio de Budapest es un factor importante para la aplicación de la Ley N° 30096.

En cuanto a especialistas en ciberdelitos, existen en solo dos dependencias Policiales especializadas en Lima y Arequipa. En cuanto a las fiscalías no existe una fiscalía especializada en delitos informáticos.

En cuanto a fiscales, todavía existe ausencia en conocimiento en la investigación y juzgamiento de los delitos informáticos, como coincide Morí Quiroz (2019).

La poca capacitación a los fiscales y operadores de justicia, hace que la Ley Nº 30096 no sea aplicada de manera correcta, como coincide Cotrina Yucra (2018).

Lo que origina transgresiones en la ley Nº 30096 Delitos Informáticos, por los jueces y fiscales, como coincide Morí Quiroz (2019).

La falta de tipificación escrita, de algunos delitos informáticos, de Ley Nº 30096 hacen que existan vacíos legales como coincide Ruiz Cruz (2016), lo cual ocasiona mala interpretación y contradicciones, como coincide Montañéz Parraga (2017).

El convenio de Budapest es un factor principal de la aplicación de la Ley Nº 30096, ya que regula internacionalmente la ciberdelincuencia, como coincide Morales Delgado (2016)**,** además de ser una herramienta útil para el derecho penal sustantivo y procesal como coincide Tenorio Pereyra (2018), que garantiza la seguridad para los ciudadanos, como coincide Mateos Pascual (2013).

La Ley Nº 30096 debe adecuarse al convenio de Budapest, debe cambiar y evolucionar como coincide Montañéz Parraga (2017), para enfrentar los ciberdelitos, es decir conforme va avanzando la tecnología en un mundo globalizado, deben avanzar las reformas y creaciones legales, como coinciden Chavarría Pérez, Jirón Vargas, & Miranda González(2016).

De lo anterior se debe a que no existe un área especializada en Delitos Informáticos, ni tampoco existe centro de investigación, en donde los peritos informáticos en delitos informáticos desarrollen habilidades y estrategias para combatir los ciberdelitos, como coinciden Aguirre Linares & Sevillano Flores (2017).

# CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

## 5.1 Conclusiones

1. Existe ineficacia ley 30096 de Delitos Informáticos, por las dificultades que se presentan al aplicar la ley 30096 de Delitos Informáticos.
2. Los ciberdelitos, en especial las ciberextorsiones están en constante crecimiento, desarrollo y evolución, por sus métodos, técnicas, herramientas perfeccionadas y sofisticas que usan los grupos organizados de ciberextorsionadores; que por sus características son ciberdelitos complejos, perjudiciales para la sociedad y un reto constante para los ejecutores de justicia y profesionales en derecho.
3. La División de Investigaciones de Delitos de Alta Tecnología (DIVINTAD) de la DIRINCRI – PNP encargada de patrullar el ciberespacio de los peruanos, no está dotada de las herramientas logísticas suficientes, ni personal necesario para combatir el delito de la ciberextorsión, ya que solo cuenta con dos dependencias en Lima y Arequipa.
4. La ley Nº 30096, no tiene reglamentación especializada en delitos informáticos, en donde se tipifiqué en forma escrita los procesos, procedimientos y pautas para combatir los ciberdelitos.
5. La ley Nº 30096 no evoluciona, ni cambia constante como las nuevas modalidades de ciberdelitos que aparecen constantemente en la actualidad.
6. El Perú se adherido al Convenio de Budapest o la Convención sobre Cibercriminalidad del Consejo de Europa que contiene reglas penales para castigar los delitos informáticos internacionalmente.
7. En el Perú, no se cuenta con un centro de investigaciones sobre ciberdelitos.

## 5.2 Recomendaciones

1. Para que la ley 30096 de Delitos Informáticos disminuya su ineficacia es recomendable crear un área especializada en Delitos Informáticos, ya que es de interés público, nacional y necesario.
2. Ante un panorama de ciberdelitos que va cambiando, evolucionando constantemente, es necesario la capacitación constaste, permanente de los ejecutores de justicia y profesionales de derecho sobre temas actuales en ciberdelitos.
3. El Estado debe implementar con herramientas logísticas y personal a la DIVINDAT para que combata los ciberdelitos, en sus diferentes modalidades, entre ellos las ciberextorsión, para que su rol que cumple de la DIVINDAT sea mucho más eficiente.
4. Para una mejor aplicación de la Ley Nº 30096, es primordial, necesario la elaboración, promulgación, publicidad de su reglamento de la Ley Nº 30096; para que los ejecutores de justicias tengan los procedimientos y pautas claras para sancionar los ciberdelitos.
5. Como los ciberdelitos cambian, evolucionan con nuevos métodos, técnicas y herramientas que usan los cibercriminales, es necesario que la Ley Nº 30096 cambie y evolucione.
6. Estando el Perú adherido al convenio de Budapest, la Ley Nº 30096 debe adecuarse a los lineamientos del convenio internacional, ajustando sus normas legales como lo están haciendo otros países que son miembros y obtener homologación al momento de aplicar sanciones a los ciberdelitos.
7. Para combatir los delitos informáticos, es importarte un centro de investigación, en donde desarrolle investigaciones sobre los ciberdelitos para prevenir y sancionar de forma correcta.

## REFERENCIAS BIBLIOGRAFÍAS


2017Análisis de los Delitos Informáticos en el actual Sistema Penal Colombiano*(Tesis para optar el Título Profesional de Abogado)*Universidad libre de ColombiaBogotá

2016Análisis de los Delitos Informáticos y su violación de los derechos constitucionales de los ciudadanos*(Tesis de pregrado para optar el título de Abogada)*Universidad Nacional de LojaLoja

*Andina -Agencia Peruana de Noticias*

*Andina- Agencia Peruana de Noticias*

2013Ciberdelincuencia Desarrollo y persecución tecnológica*(Tesis de Pregrado para optar el Título Profesional de Telemática)*Universidad Politécnica de MadridMadrid

*Comentarios a la parte especial del Derecho Penal*2016PamplonaAranzadi

Congreso de la República*Congreso de la República*

Consejo Nacional de Política Criminal CONAPOC2020*Diagnóstico Situacional Multisectorial sobre la ciberdelincuencia en el Perú*LimaMinisterio de Justicia y Derechos Humanos - Observatorio Nacional de Política Criminal

Delitos Informáticos2014*IUS ET VERITAS*286-287

2014Delitos Informáticos y el rol de La División de Investigación de Delitos de Alta Tecnología PNP, Lima. 2013*(Tesis en Maestría en Desarrollo y Defensa Nacional)*Centro de Altos Estudios Nacionales, CAEM de Perú.Lima

Sin Fecha*Delitos Informáticos, Optica Policial*LimaDivisión de Investigación de Delitos de Alta Tecnología

*Derecho Informático*2009México D.F.Mc Graw Hill

*Derecho Penal - Parte Especial*2007Buenos AiresAstrea

*Derecho Penal Peruano, Parte Especial*1974LimaInstituto Peruano de Ciencias Penales

2017Desafíos a enfrentar en la Aplicación de Leyes sobre delitos infórmaticos en el Salvador*(Tesis de Maestro en Seguridad y Gestión Informáticos)*Universidad Don Bosco de el SalvadorEl Salvador

2018Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest

sobre la Ciberdelincuencia*(Tesis de Maestría en Diplomacía y Relaciones Internacionales*Academia Diplomática del Perú. Javier Pérez de CuéllarLima

*Diccionario de Derecho Penal*2000LimaImportadores S.A.

*Diccionario Enciclopédico de Derecho Usual*2008Buenos AriesHeliasta S.R.L.

DIRINCRI PNPDIVINDAT2019*INFORME Nº 105-DIRINCRI PNP/DIVINDAT/SEC*LimaPolícia Nacional del Perí

DIVINDAT2019División de Delitos de Alta Tecnología*Polícia Nacional del Perú*10-11

DIVINDAT*Organigrama DIVINDAT [Imagen]*

2015El delito en la cibersociedad y la justicia penal internacional*(Tesis de Doctorado en Derecho)*Universidad Compultense de MadridMadrid

Eleven PathsTelefónica2016*La ciberextosión, una industria en crecimiento*EspañaEleven Paths

Evolución de la extorsión en México: un análisis estadístico regional (2012-2013)2015*Revista Mexicana de Opinión Pública*119

Fortinet Threat *Threat Intelligence Insider Latin America de Fortinet*

FreepikSin Fecha*Phishing account concept [Imagen]*

Fundación Heinrich Böll México y El Caribe2013*Ponencia Marco Lara Klahr*

Fundación Ideas para la Paz2012*Extorsión y empresas en Colombia. Guía práctica para enfrentar el delito de la extorsión desde la empresa privada.*BogotáFundación Ideas para la Paz

2016La Ciberdelincuencia y su regulación Jurídica en Centroamérica con énfasis en Costa Rica, El Salvador y Nicaragua*(Tesis para optar el Título Profesional de Abogado)*Universidad Nacional Autónoma de Nicaragua UNAN-LeónLeón

2016La Inseguridad al utilizar los servicios de Redes Sociales y la Problemática Judicial para regular los Delitos Informáticos en el Perú-2015*(Tesis de Pregrado para optar el Título Profesional de Abogado)*Universidad Señor de SipánPimentel

Ley Nº 30999 - Ley de Ciberdefensa*Diario el Peruano*9

2019Los Delitos Informáticos y la Protección Penal de la intimidad en el Distrito Judicial de Lima periodo 2008 Al 2012*(Tesis de Maestría en Derecho Penal)*Universidad Nacional Federico VillarrealLima

2018Los factores principales que impiden la aplicación de la Ley N°30171- Lima Norte en el año 2016*(Tesis de Pregrado para optar el título Profesional de Abogado)*Universidad César VallejoLima

MacrovectorSin fecha*Hacker icon set with different types of hackers stealing information breaking computer system [Imagen]*

MacrovectorSin fecha*Internet hacker security composition set Free Vector [Imagen]*

Mazuelos Coello, Juan2007Modelos de imputación en el Derecho Penal Informático*Derecho Penal y criminología*40-41

Ministerio de Justicia y Derechos Humanos2015*Sistema Peruano de Información Jurídica*

Ministerio de JusticiaSistema Peruano de Información Jurídica*Congreso de la República*

Ministerio de Relaciones ExterioresConvenio sobre la delincuencia. Budapest, 23 XI 2001*Diario el Peruano*2

Ministerio Público - Fiscalía de la Nación2018*Boletín Estadístico del Ministerio Público Diciembre 2017*LimaMinisterio Público - Fiscalía de la Nación

Ministerio Público - Fiscalía de la Nación2018*Boletín Estadístico del Ministerio Público Diciembre 2017*LimaMinisterio Público - Fiscalía de la Nación

Ministerio Público - Fiscalía de la Nación2018*Boletín Estadístico Julio 2018*LimaMinisterio Público - Fiscalía de la Nación Oficina de Racionalización y Estadística

Ministerio Público - Fiscalía de la Nación2019*Boletín Estadístico Diciembre 2018*LimaMinisterio Público

Ministerio Público - Fiscalía de la Nación2020*Boletín Estadístico del Ministerio Público Julio 2020*LimaMinisterio Público - Fiscalía de la NaciónOficina de Racionalización y Estadística

Oficina de Seguridad del Internauta*¿Quiénes son los ciberdelincuentes y qué buscan? [Infografía]*

Panda Security*Panda Security Mediacenter*

Presidencia del Consejo de Ministros*Congreso de la República*

Presidencia del Consejo de MinistrosSecretaria de Gobierno Digital2020*Alerta*

*Integrada de Seguridad Digital Nº 016-2020-PECERT*LimaPECERT

Presidencia del Consejo de MinistrosSecretaria de Gobierno Digital2020*Alerta Integrada de Seguridad Digital Nº 256-2020-PECERT*LimaPECERT

*Prevención Delitos Informáticos y cometidos a través de la Tecnología*

Real Academia Española2020*Diccionario de la lengua española*

2020*Riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte de Ciberseguridad 2020*Observatorio Ciberseguridad

Statista*¿Cómo funciona un ransomware? [Imagen]*

Tecnología clic*Revista de Técnología. ciencia, informática, internet y más*

*Tendencias Cibercrimen Colombia 2019-2020*

Trend Micro2015*Sextortion in the far east*TexasTrend Micro Incorporated

Universidad de GuadalajaraSin Fecha*Protocolo de seguridad para la extorsión telefónica [Infografía]*

**ANEXOS**

## Anexo A: LEY N° 30096



PODER LEGISLATIVO

CONGRESO DE LA REPUBLICA

### LEY Nº 30096

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

El Congreso de la República
Ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;
Ha dado la Ley siguiente:

### LEY DE DELITOS INFORMÁTICOS

#### CAPÍTULO I

#### FINALIDAD Y OBJETO DE LA LEY

**Artículo 1. Objeto de la Ley**
La presente Ley 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.

#### CAPÍTULO II

#### DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS

**Artículo 2. Acceso ilícito**
El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.
Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.

**Artículo 3. Atentado contra la integridad de datos informáticos**
El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles 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.

**Artículo 4. Atentado contra la integridad de sistemas informáticos**

El que, a través de las tecnologías de la información o de la comunicación, 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.

## CAPÍTULO III

## DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES

**Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos**

El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

## CAPÍTULO IV

## DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

**Artículo 6. Tráfico ilegal de datos**

El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

**Artículo 7. Interceptación de datos informáticos**

El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

## CAPÍTULO V

## DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

**Artículo 8. Fraude informático**

El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

## CAPÍTULO VI

## DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA

**Artículo 9. Suplantación de identidad**

El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

## CAPÍTULO VII

## DISPOSICIONES COMUNES

**Artículo 10. Abuso de mecanismos y dispositivos informáticos**

El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, especificamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

**Artículo 11. Agravantes**

El juez aumenta la pena privativa de libertad hasta cualquiera de los delitos previstos en la presente Ley cuando:

1. El agente comete el delito en calidad de integrante de una organización criminal.
2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.
3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.
4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

## DISPOSICIONES COMPLEMENTARIAS FINALES

**PRIMERA. Codificación de la pornografía infantil**

La Policía Nacional del Perú puede mantener en sus archivos, con la autorización y supervisión respectiva del Ministerio Público, material de pornografía infantil, en medios de almacenamiento de datos informáticos, para fines exclusivos del cumplimiento de su función. Para tal efecto, cuenta con una base de datos debidamente codificada.

La Policía Nacional del Perú y el Ministerio Público establecen protocolos de coordinación en el plazo de treinta días a fin de cumplir con la disposición establecida en el párrafo anterior.

**SEGUNDA. Agente encubierto en delitos informáticos**

El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.

**TERCERA. Coordinación interinstitucional de la Policía Nacional del Perú con el Ministerio Público**

La Policía Nacional del Perú fortalece al órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, la Policía Nacional del Perú centraliza la información aportando su experiencia en la elaboración de los programas y acciones para

la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad.

**CUARTA. Cooperación operativa**
Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reforzada en el plazo de treinta días desde la vigencia de la presente Ley.

**QUINTA. Capacitación**
Las instituciones públicas involucradas en la prevención y represión de los delitos informáticos deben impartir cursos de capacitación destinados a mejorar la formación profesional de su personal –especialmente de la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial– en el tratamiento de los delitos previstos en la presente Ley.

**SEXTA. Medidas de seguridad**
La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) promueve permanentemente, en coordinación con las instituciones del sector público, el fortalecimiento de sus medidas de seguridad para la protección de los datos informáticos sensibles y la integridad de sus sistemas informáticos.

**SÉTIMA. Buenas prácticas**
El Estado peruano realiza acciones conjuntas con otros Estados a fin de poner en marcha acciones y medidas concretas destinadas a combatir el fenómeno de los ataques masivos contra las infraestructuras informáticas y establece los mecanismos de prevención necesarios, incluyendo respuestas coordinadas e intercambio de información y buenas prácticas.

**OCTAVA. Convenios multilaterales**
El Estado peruano promueve la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de los delitos informáticos.

**NOVENA. Terminología**
Para efectos de la presente Ley, se entenderá, de conformidad con el artículo 1 del Convenio sobre la Ciberdelincuencia, Budapest, 23.XI.2001:

a. **Por sistema informático:** todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.
b. **Por datos informáticos:** toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

**DÉCIMA. Regulación e imposición de multas por la Superintendencia de Banca, Seguros y AFP**
La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5 del artículo 235 del Código Procesal Penal, aprobado por el Decreto Legislativo 957.
El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.

**UNDÉCIMA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones**
El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por el Decreto Legislativo 957.
El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.

## DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

**PRIMERA. Modificación de la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional**
Modifícase el artículo 1 de la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional, modificado por el Decreto Legislativo 991, en los siguientes términos:

"**Artículo 1. Marco y finalidad**
La presente Ley tiene por finalidad desarrollar legislativamente la facultad constitucional otorgada a los jueces para conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional.
Solo podrá hacerse uso de la facultad prevista en la presente Ley en los siguientes delitos:

1. Secuestro.
2. Trata de personas.
3. Pornografía infantil.
4. Robo agravado.
5. Extorsión.
6. Tráfico ilícito de drogas.
7. Tráfico ilícito de migrantes.
8. Delitos contra la humanidad.
9. Atentados contra la seguridad nacional y traición a la patria.
10. Peculado.
11. Corrupción de funcionarios.
12. Terrorismo.
13. Delitos tributarios y aduaneros.
14. Lavado de activos.
15. Delitos informáticos."

**SEGUNDA. Modificación de la Ley 30077, Ley contra el crimen organizado**
Modifícase el numeral 9 del artículo 3 de la Ley 30077, Ley contra el crimen organizado, en los siguientes términos:

"**Artículo 3. Delitos comprendidos**
La presente Ley es aplicable a los siguientes delitos:
(...)
9. Delitos informáticos previstos en la ley penal."

**TERCERA. Modificación del Código Procesal Penal**
Modifícase el numeral 4 del artículo 230, el numeral 5 del artículo 235 y el literal a) del numeral 1 del artículo 473 del Código Procesal Penal, aprobado por el Decreto Legislativo 957, en los siguientes términos:

"**Artículo 230. Intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación**
(...)
4. Los concesionarios de servicios públicos de telecomunicaciones deberán facilitar, en el plazo máximo de treinta días hábiles, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones, así como la información sobre la identidad de los titulares del servicio, los números de registro del cliente, de la línea telefónica y del equipo, del tráfico de llamadas y los números de protocolo de internet, que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida,

las veinticuatro horas de los trescientos sesenta y cinco días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento. Los servidores de las indicadas empresas deberán guardar secreto acerca de las mismas, salvo que se les citare como testigos al procedimiento. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular.

Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, cuando por razones de innovación tecnológica los concesionarios renueven sus equipos o software, se encontrarán obligados a mantener la compatibilidad con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú.

**Artículo 235. Levantamiento del secreto bancario**

(...)

5. Las empresas o entidades requeridas con la orden judicial deberán proporcionar, en el plazo máximo de treinta días hábiles, la información correspondiente o las actas y documentos, incluso su original, si así se ordena, y todo otro vínculo al proceso que determine por razón de su actividad, bajo apercibimiento de las responsabilidades establecidas en la ley. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular.

**Artículo 473. Ámbito del proceso y competencia**

1. Los delitos que pueden ser objeto de acuerdo, sin perjuicio de los que establezca la Ley, son los siguientes:

a) Asociación ilícita, terrorismo, lavado de activos, delitos informáticos, contra la humanidad;"

**CUARTA. Modificación de los artículos 162, 183-A y 323 del Código Penal**

Modifícanse los artículos 162, 183-A y 323 del Código Penal, aprobado por el Decreto Legislativo 635, en los siguientes términos:

"**Artículo 162. Interferencia telefónica**

El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

**Artículo 183-A. Pornografía infantil**

El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por videos o audios, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a personas de catorce y menos de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años y con ciento veinte a trescientos sesenta y cinco días multa.

La pena privativa de libertad será no menor de diez ni mayor de doce años y de cincuenta a trescientos sesenta y cinco días multa cuando:

1. El menor tenga menos de catorce años de edad.
2. El material pornográfico se difunda a través de las tecnologías de la información o de la comunicación.

Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 173 o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil, la pena privativa de libertad será no menor de doce ni mayor de quince años. De ser el caso, el agente será inhabilitado conforme a los numerales 1, 2 y 4 del artículo 36.

**Artículo 323. Discriminación**

El que, por sí o mediante terceros, discrimina a una o más personas o grupo de personas, o incita o promueve en forma pública actos discriminatorios, por motivo racial, religioso, sexual, de factor genético, filiación, edad, discapacidad, idioma, identidad étnica y cultural, indumentaria, opinión política o de cualquier índole, o condición económica, con el objeto de anular o menoscabar el reconocimiento, goce o ejercicio de los derechos de la persona, será reprimido con pena privativa de libertad no menor de dos años ni mayor de tres o con prestación de servicios a la comunidad de sesenta a ciento veinte jornadas.

Si el agente es funcionario o servidor público, la pena será no menor de dos ni mayor de cuatro años e inhabilitación conforme al numeral 2 del artículo 36.

La misma pena privativa de libertad señalada en el párrafo anterior se impondrá si la discriminación se ha materializado mediante actos de violencia física o mental, o si se realiza a través de las tecnologías de la información o de la comunicación."

**DISPOSICIÓN COMPLEMENTARIA DEROGATORIA**

**ÚNICA. Derogatoria**

Deróganse el numeral 3 del segundo párrafo del artículo 186 y los artículos 207-A, 207-B, 207-C y 207-D del Código Penal.

Comuníquese al señor Presidente Constitucional de la República para su promulgación.

En Lima, a los veintisiete días del mes de setiembre de dos mil trece.

FREDY OTÁROLA PEÑARANDA
Presidente del Congreso de la República

MARÍA DEL CARMEN OMONTE DURAND
Primera Vicepresidenta del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiún días del mes de octubre del año dos mil trece.

OLLANTA HUMALA TASSO
Presidente Constitucional de la República

JUAN F. JIMÉNEZ MAYOR
Presidente del Consejo de Ministros

**1003117-1**

## Anexo B: LEY N° 30171

FUNDADO EL 22 DE OCTUBRE DE 1825 POR EL LIBERTADOR SIMÓN BOLÍVAR

El Peruano

www.elperuano.pe | DIARIO OFICIAL

AÑO DE LA PROMOCIÓN DE LA INDUSTRIA RESPONSABLE Y DEL COMPROMISO CLIMÁTICO

Lunes 10 de marzo de 2014

# NORMAS LEGALES



### LEY Nº 30171

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

LA COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

### LEY QUE MODIFICA LA LEY 30096, LEY DE DELITOS INFORMÁTICOS

**Artículo 1. Modificación de los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos**

Modifícanse los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos, en los siguientes términos:

"**Artículo 2. Acceso ilícito**

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado."

"**Artículo 3. Atentado a la integridad de datos informáticos**

El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles 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."

"**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."

"**Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos**

El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal."

"**Artículo 7. Interceptación de datos informáticos**

El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de

un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.
La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.
La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.
Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores."

"**Artículo 8. Fraude informático**
El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa.
La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social."

"**Artículo 10. Abuso de mecanismos y dispositivos informáticos**
El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa."

**Artículo 2. Modificación de la tercera, cuarta y undécima disposiciones complementarias finales de la Ley 30096, Ley de Delitos Informáticos**
Modifícanse la tercera, cuarta y undécima disposiciones complementarias finales de la Ley 30096, Ley de Delitos Informáticos, en los siguientes términos:

"**TERCERA. Coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados**
La Policía Nacional del Perú fortalece el órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, el centro de respuesta temprana del gobierno para ataques cibernéticos (Pe-CERT), la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) y los Organismos Especializados de las Fuerzas Armadas, la Policía Nacional centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad."

"**CUARTA. Cooperación operativa**
Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial, el Pe-CERT (Centro de respuesta temprana del gobierno para ataques cibernéticos), la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática), Organismos Especializados de las Fuerzas Armadas y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reformada en el plazo de treinta días desde la vigencia de la presente Ley."

"**UNDÉCIMA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones**
El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece las multas aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por Decreto Legislativo 957.
Las empresas de telecomunicaciones organizan sus recursos humanos y logísticos a fin de cumplir con la debida diligencia y sin dilación la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal.
El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa a fin de que el Organismo Supervisor de Inversión Privada en Telecomunicaciones aplique la multa correspondiente."

**Artículo 3. Incorporación del artículo 12 a la Ley 30096, Ley de Delitos Informáticos**
Incorpórase el artículo 12 a la Ley 30096, Ley de Delitos Informáticos, en los siguientes términos:

"**Artículo 12. Exención de responsabilidad penal**
Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos."

**Artículo 4. Modificación de los artículos 158, 162 y 323 del Código Penal**
Modifícanse los artículos 158, 162 y 323 del Código Penal, aprobado por Decreto Legislativo 635 y modificado por la Ley 30096, Ley de Delitos Informáticos, en los siguientes términos:

"**Artículo 158. Ejercicio de la acción penal**
Los delitos previstos en este Capítulo son perseguibles por acción privada, salvo en el caso del delito previsto en el artículo 154-A."

"**Artículo 162. Interferencia telefónica**
El que, indebidamente, interfiere o escucha una conversación telefónica o similar, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.
Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.
La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.
La pena privativa de libertad será no menor de ocho ni mayor de diez años, cuando el delito comprometa la defensa, seguridad o soberanía nacionales.
Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores."

"**Artículo 323. Discriminación e incitación a la discriminación**
El que, por sí o mediante terceros, discrimina a una o más personas o grupo de personas, o incita o promueve en forma pública actos discriminatorios, por motivo racial, religioso, sexual, de factor genético, filiación, edad, discapacidad, idioma, identidad étnica y cultural, indumentaria, opinión política o de cualquier índole, o condición económica, con el objeto de anular o menoscabar el reconocimiento, goce o ejercicio de los derechos de la persona, será reprimido con pena privativa de libertad no menor de dos años, ni mayor de tres o con prestación de servicios a la comunidad de sesenta a ciento veinte jornadas.
Si el agente es funcionario o servidor público la pena será no menor de dos, ni mayor de cuatro años e inhabilitación conforme al numeral 2 del artículo 36.
La misma pena privativa de libertad señalada en el párrafo anterior se impondrá si la discriminación, la incitación o promoción de actos discriminatorios se ha materializado mediante actos de violencia física o mental o a través de internet u otro medio análogo."

**Artículo 5. Incorporación de los artículos 154-A y 183-B al Código Penal**
Incorpóranse los artículos 154-A y 183-B al Código Penal, aprobado por Decreto Legislativo 635, con el siguiente texto:

"**Artículo 154-A. Tráfico ilegal de datos personales**
El que ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera

personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años.
Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en el párrafo anterior."

"**Artículo 183-B. Proposiciones sexuales a niños, niñas y adolescentes**
El que contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36.
Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36."

**Artículo 6. Modificación del numeral 4 del artículo 230 del Código Procesal Penal**
Modifícase el numeral 4 del artículo 230 del Código Procesal Penal, modificado por la Ley 30096, Ley de Delitos Informáticos, con el siguiente texto:

"**Artículo 230. Intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles**
(...)

4. Los concesionarios de servicios públicos de telecomunicaciones deben facilitar, en forma inmediata, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las 24 horas de los 365 días del año, bajo apercibimiento de ser pasible de las responsabilidades de Ley en caso de incumplimiento. Los servidores de las indicadas empresas deben guardar secreto acerca de las mismas, salvo que se les citare como testigo al procedimiento.
Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, cuando por razones de innovación tecnológica los concesionarios renueven sus equipos y software, se encontrarán obligados a mantener la compatibilidad con el sistema de intervención y control de las comunicaciones de la Policía Nacional del Perú.
(...)."

**DISPOSICIÓN COMPLEMENTARIA DEROGATORIA**

**ÚNICA. Derogación del artículo 6 de la Ley 30096, Ley de Delitos Informáticos**
Derógase el artículo 6 de la Ley 30096, Ley de Delitos Informáticos.

Comuníquese al señor Presidente Constitucional de la República para su promulgación.

En Lima, a los diecisiete días del mes de febrero de dos mil catorce.
FREDY OTÁROLA PEÑARANDA
Presidente del Congreso de la República

JOSÉ LUNA GÁLVEZ
Tercer Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL
DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los nueve días del mes de marzo del año dos mil catorce.

OLLANTA HUMALA TASSO
Presidente Constitucional de la República

RENÉ CORNEJO DÍAZ
Presidente del Consejo de Ministros

**1059231-2**